(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2002 (30.05.2002)

PCT

(10) International Publication Number
WO 02/43322 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/US01/48047

(22) International Filing Date: 26 October 2001 (26.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/244,630 31 October 2000 (31.10.2000) US
09/817,993 27 March 2001 (27.03.2001) US

(71) Applicant: MARCONI COMMUNICATIONS, INC. [US/US]; 5900 Landerbrook Drive, Cleveland, OH 44124 (US).

(72) Inventor: TORNAR, Massimiliano; 2765 Rue Notre Dame 101, Lachine, Quebec H8S 2H3 (CA).

(74) Agents: FEELING, Drexel, F. et al.; Jones, Day, Reavis & Pogue, North Point, 901 Lakeside Avenue, Cleveland, OH 44114 (US).

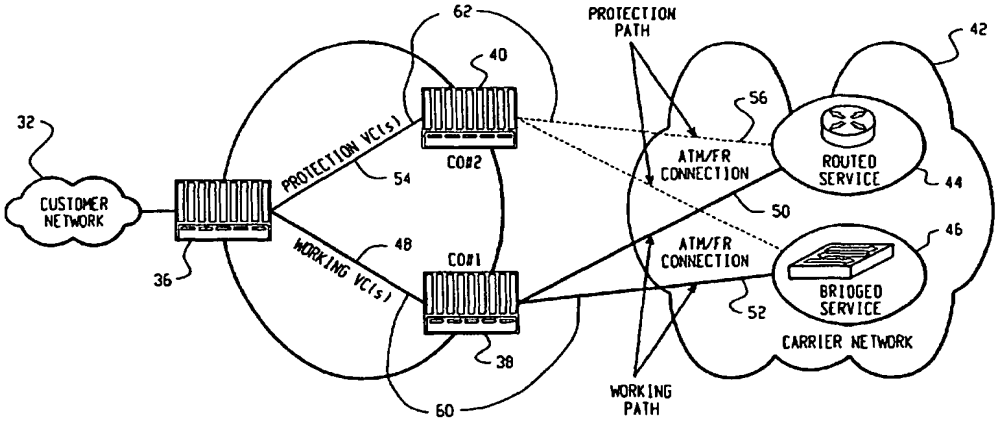
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: IP MULTI-HOMING



(57) Abstract: A method and system for providing a customer network with high speed access to a carrier network is provided. The system comprises an access device for providing a communication path for the customer network, a first concentrator device that is operable to establish a communication path with the carrier network, and a second concentrator device that is operable to establish a communication path with the carrier network. The access device is operable to receive data traffic from the customer network and to forward the data traffic within the system. The access device and the first concentrator device cooperate to form a first virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the first virtual channel is the primary communication channel for the customer network. The access device and the second concentrator device cooperate to form a second virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the second virtual channel is a backup communication channel for the customer network. The system is operable to switch the primary communication channel from the first virtual channel to the second virtual channel upon detection of a failure in the first virtual channel.

WO 02/43322 A2

IP MULTI-HOMING

This application claims the benefit under 35 U.S.C. § 119(e) to copending U.S. Provisional Patent Application No. 60/244630 entitled "IP Multi-Homing" and filed on October 31, 2000. This application also incorporates copending U.S. Provisional Patent Application No. 60/244630 by reference as if fully rewritten here.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention is directed toward the field of data communication networks. In particular, the invention is directed to a system and method for providing protected communication paths between a LAN and a carrier network.

2. Description of the Related Art

Figure 1 sets forth a schematic drawing of a communication system **2** that provides a user or a user's local area network **3** ("LAN") with access to the internet or some other wide area network ("WAN"). In the embodiment shown, a LAN **3** is provided with internet access through a fiber optic system **4**. The fiber optic system **4** provides a connection between the user LAN **3** and an internet access device such as an internet backbone router **5** ("BR"). The BR **5** has a number of ports (not shown) with internet protocol ("IP") addresses assigned thereto. Internet access is achieved through accessing the ports on the BR **5**.

The preferred user LAN **3** is an Ethernet LAN but other LAN types such as token ring, FDDI, etc., could be used. LAN Hosts **7b** preferably are personal computers ("PCs") but optionally could be servers or other computer or communication equipment. LAN router **7a** preferably comprises computer or communication hardware that forwards data from or to other computer or communication equipment on the LAN **3**. LAN router **7a** optionally could be

coupled to other subnets (not shown) on the user's premises which interconnect other LAN hosts (not shown).

Figure 2 sets forth a more detailed view of an exemplary communication system **2** for providing a plurality of user LANs **3** with access to the internet or other WAN via a fiber optic system. The exemplary communication system **2** includes a fiber optic system that preferably is arranged in a ring network **10** and more preferably in a Synchronous Optical Network ("SONET") or SDH ring. The communication system **2** also includes a plurality of network nodes **12a, 12b, 12c, & 12d** that are coupled together in the SONET/SDH ring **10**, a plurality of local or user LANs **3a, 3b & 3c** that are coupled to the network nodes **12a, 12b & 12c**, respectively, preferably via fiber optic cables **15**, and an internet or WAN access device **5** such as an internet backbone router ("BR") coupled to network node **12d**.

Figure 3 sets forth a system diagram of a preferred SONET/SDH ring **20** for use in a communication system that practices the present invention. The SONET/SDH ring **20** includes a plurality of network nodes **22**, labeled **N0-N3**, coupled in a ring structure by one or more communication paths **24A, 24B**. As shown in FIG. 3, the two paths **24A, 24B** transport SONET/SDH data streams (many packets/cells) in opposite directions about the ring (*i.e.*, east and west). The communication paths **24A, 24B** are preferably fiber optic connections (in SONET/SDH), but could, alternatively be electrical paths or even wireless connections (in other types of ring networks). In the case of a fiber optic connection, paths **24A, 24B** could be implemented on a single fiber **24**, on dual fibers **24A, 24B**, or some other combination of connections. Each network node **22** is preferably coupled to two other network nodes **22** in the ring structure **20**. For example, network node **N0** is coupled to network nodes **N1** and **N3**. The coupling between the nodes in FIG. 3 is two-way, meaning that each node **22** transmits and receives data (packets/cells) to and from each of the two other nodes **22** to which it is connected. Each network node **22** includes at least two

transmitter/receiver interfaces, one for each connection to another node **22**. The network nodes **22** could be many types of well-known network devices, such as add-drop multiplexers ("ADMs"), switches, routers, cross-connects or other types of devices. The devices **22** shown in FIG. 3 are preferably ADMs. An ADM is a three terminal device having a local add/drop interface, an upstream network node interface, and a downstream network node interface. These ADMs **22** are coupled to local nodes **26**, and are used to add packets/cells from the local nodes **26** to the SONET/SDH data stream, and conversely to drop packets from the SONET/SDH data stream to the local nodes **26**. A system and method for packet transport in a SONET/SDH ring network and an exemplary ADM is described in more detail in commonly-assigned United States Patent Application S/N 09/378,844 ("the '844 application"), which is incorporated herein by reference. For more information on SONET/SDH formats, line-speeds, and theory of operation, see John Bellamy, *Digital Telephony*, 2d Edition (1991), pp. 403-425.

The network nodes **22** shown in FIG. 3 may be logically connected by a plurality of virtual paths that coexist on the physical network connection(s) **24**. Virtual paths are also known as logical paths or "pipes." For example, although there is only one physical connection from node **N0** to node **N1** to node **N2**, there may be numerous virtual paths between these nodes, such as one virtual path from **N0** to **N1**, another from **N0** to **N2** and another from **N1** to **N2**. Each virtual path may include a plurality of virtual channels, wherein each virtual channel transports packets (or cells) formatted according to the SONET/SDH SPE. The use of virtual paths in SONET/SDH ring networks is described in more detail in commonly-assigned United States Patent Application S/N 09/324,244 ("the '244 application"), which also is incorporated herein by reference.

In the exemplary communication system **2** shown in Figure 2, the network nodes **12a, 12b & 12c** are access nodes. The network devices that make up access nodes **12a, 12b & 12c** each include an access device or access card ("AC") **14**. Each access card **14** is operable to transfer data packets between a

user's equipment on a LAN **3** and other nodes **12** on the ring network **10**. The access cards **14** of the present invention may physically reside within a network device of the SONET/SDH ring **10** or alternatively may be coupled to a network device.

The network node **12d** of the exemplary communication system **2** is an internet gateway node and the network device that makes up the gateway node **12d** includes a multiplexor device or concentrator card ("CC") **16**. The CC **16** functions as a switch that multiplexes data packets transmitted by the access nodes **12a, 12b & 12c** onto a single data transmission channel **18** for further routing to the internet access device **5**. The CC **16** also functions as a switch for forwarding data packets received over the data transmission channel **18** from the internet access device **5** to one or more access nodes **12a, 12b** or **12c**.

Router ports have been configured for shared use between multiple virtual circuits and sub-interfaces. The concentrator card **16** facilitates the shared use of a router port and has a two-fold role. The concentrator card **16** merges the data from the various LANs **3** and access cards **14** on the ring network into a single pipe for forwarding to the single router port of the BR **5** to which the concentrator card **16** is coupled. In merging the data, the concentrator card **16** couples the data to different interfaces within the router port. The concentrator card's **16** second task is to take data from the BR **5**, packet by packet, and forwards the data to the various access nodes **12** on the ring network.

Each access card **14** includes at least one protocol engine **30**, as shown in Figure 4, for providing a fiber extended router port **6** to a LAN **3**. The protocol engine **30** provides a permanent address for use by the LAN devices **7** when transmitting data packets to the WAN. The protocol engine **30** reformats data packets from the LAN devices **7** and transmits the reformatted data packets over the ring **10** through the concentrator interface of CC **16** to a sub-interface of BR **5**. The protocol engine **30** also receives data packets from a sub-interface of BR **5** through the concentrator interface and reformats those data packets to the

format used on the LAN 3. The protocol engine 30 addresses at least three main architectural issues: encapsulation, maximum transfer unit ("MTU"), and address resolution. The use of protocol engines and Access Cards in SONET/SDH ring networks are described in more detail in commonly-assigned United States Patent Application S/N 09/514,032 ("the '032 application"), which also is incorporated herein by reference.

If there is only one concentrator node for the entire network and there is a malfunction in that concentrator node or in a virtual path to that concentrator node, then wide area network access for one or more nodes in that network may be interrupted.

Therefore, there remains a need in this art for a method and system for providing protected virtual paths between local area networks (LANs) and wide area networks (WANs). There remains a particular need for a method and system for detecting malfunctions in a primary virtual path and for switching to the protection virtual path when a malfunction is detected. There also remains a more particular need for a method and a system that can provide protected virtual paths in a manner that minimally impacts the user computer equipment on a LAN connected to the network node on the system.

SUMMARY OF THE INVENTION

The present invention provides protected virtual paths to a customer network or LAN by providing access to a carrier network via a plurality of virtual channels. The present invention provides a mechanism for detecting failures associated with the virtual channels and a mechanism for switching from a failed virtual channel to a protection virtual channel upon detection of a failure.

The present invention provides many advantages over the presently known communication systems for providing access to a carrier network. Not all of these advantages are simultaneously required to practice the invention as claimed, and the following list is merely illustrative of the types of benefits that

may be provided, alone or in combination, by the present invention. These advantages include: (1) the overall architecture of the network, with the concentrator interfaces connected to the carrier network at two different redundant locations, and the interaction between the carrier network devices (routers and bridges) and the system according to the present invention; (2) the concentrator device failure detection capability in the access device; (3) the Backbone Router failure detection capability and consequent triggering of VC switching; (4) IP layer faults detection and reporting to the access device; and (5) ATM layer fault detection and reporting to the access device.

In accordance with the present invention, a method and system for providing a customer network with high speed access to a carrier network is provided. The system comprises an access device for providing a communication path for the customer network, a first concentrator device that is operable to establish a communication path with the carrier network, and a second concentrator device that is operable to establish a communication path with the carrier network. The access device is operable to receive data traffic from the customer network and to forward the data traffic within the system. The access device is also operable to receive data traffic from the system and to drop some of the data traffic to the customer network. The first concentrator device is operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic. The second concentrator device is also operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic. The access device and the first concentrator device cooperate to form a first virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the first virtual channel is the primary communication channel for the customer network. The access device and the second concentrator device cooperate to form a second virtual channel for

allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the second virtual channel is a backup communication channel for the customer network. The system is operable to switch the primary communication channel from the first virtual channel to the second virtual channel upon detection of a failure in the first virtual channel.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will become more apparent from the following description when read in conjunction with the accompanying drawings wherein:

Fig. 1 is a schematic drawing of a communication system having a fiber extended router port;

Fig. 2 is a schematic drawing of a communication system that provides multiple LANs with access to a WAN via a ring network;

Fig. 3 is a schematic drawing of an optical ring network used in a preferred embodiment of the invention;

Fig. 4 is a schematic view of a communication system that provides multiple LANs with access to a WAN;

Fig. 5 is a schematic diagram of a network that provides redundant concentrator interfaces;

Fig. 6 is a schematic drawing of a network illustrating the transmission of traffic via a working virtual channel;

Fig. 7 is a schematic drawing of a network illustrating the transmission of traffic via the protection virtual channel after a failure has been detected;

Fig. 8 is a schematic drawing of a network illustrating active detection of router failures;

Fig. 9 is a diagram illustrating concentrator card failure detection by the protection concentrator card;

Fig. 10 is a schematic drawing of a network illustrating concentrator card failure detection by the access card;

Fig. 11 is a state diagram illustrating the access card path switching algorithm;

Fig. 12 is a schematic diagram illustrating virtual channel switching after the protection concentrator card detects a failure in the working virtual channel;

Fig. 13 is a schematic drawing illustrating virtual channel switching after the working concentrator card notifies the access card of a failure;

Fig. 14 is a schematic drawing illustrating virtual channel switching after the working concentrator card notifies the access card of a failure;

Fig. 15 is a state diagram of a revertive algorithm in the access card;

Fig. 16 is a state diagram of a non-revertive algorithm in the access card;

Fig. 17 is a schematic diagram illustrating a system with an asymmetric configuration;

Fig. 18 is a schematic diagram illustrating a system with a symmetric configuration;

Fig. 19 is a schematic diagram illustrating the impact of the present invention on a customer LAN;

Fig. 20 is a schematic diagram of an alternate embodiment illustrating the impact of the present invention on a customer LAN;

Fig. 21 is a schematic drawing illustrating the use of the present invention with a user network having a firewall; and

Fig. 22 is a schematic drawing illustrating the use of the present invention with a user network with a screened subnet firewall.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a system for protecting against a loss of services by providing protection virtual channels.

A. **Multi-homed Reference Network**

In a preferred embodiment, a user or customer LAN **32** is connected via a ring **34** and a network node device **36** to two Central Offices (CO) **38, 40**, as shown in Figure 5. To interface with the user LAN **32**, the network node device **36** preferably includes an access card **14** which preferably provides an Ethernet port as the interface for the user LAN **32**. The central offices **38, 40** connect the ring **34** to the global carrier network **42**. The central offices **38, 40** preferably include a concentrator card **16** that interfaces with and provides the connection to the carrier network **42**. The carrier network **42** provides routed services **44** and bridged services **46** for allowing devices coupled to the ring **34** to connect and transport data packets to and from WANs or the internet. The protection switching mechanism offered by the present invention ensures that if there is a failure of either the CO#1 **38** equipment or the link connecting the CC in CO#1 **38** to the carrier network **42**, then all the traffic is delivered from and to the CO#2 **40**. The present invention also provides a mechanism whereby the routed services **44** and the bridged services **46** provided by the carrier **42** are made available even in the case of failure of one of the two COs **38, 40**.

The ring **34** of the preferred embodiment includes two or more network node devices. Two of the network node devices are COs preferrably having CCs **16** for connecting to a carrier network **42**. One of the network node devices is coupled to a user LAN and preferably includes an AC **14** for providing the coupling. The network node device that is coupled to the user LAN preferably is not one of the COs but optionally could be one of the COs. One skilled in the art could configure the ring **34** in a number of configurations without departing from the scope of the present invention.

As shown in Figure 6, to make the routed services **44** and the bridged services **46** available on a protected basis, provided are a working virtual channel

("VC") **48**, a routed services working ATM virtual channel **50**, a bridged services working ATM virtual channel **52**, at least one protection VC **54**, at least one routed services protection ATM virtual channel **56**, and at least one bridged services protection ATM virtual channel **58**. Therefore, the user LAN **32** is provided with routed service **44** and bridged service **46** in the carrier network **42** via a working VC **48** to CO #1 **38** and working ATM virtual channels **50** and **52** to routed service **44** and bridged service **46**, respectively. In addition, the user LAN **32** is provided with routed service **44** and bridged service **46** in the carrier network **42** via a protection VC **54** to CO #2 **40** and protection ATM virtual channels **56** and **58** to routed service **44** and bridged service **46**, respectively. The working VC **48** and working ATM virtual channels **50** and **52** shall be referred hereinafter as working PVC **60**, and the protection VC **54** and working paths **56** and **58** shall be referred hereinafter as protection PVC **62**. The protection PVC **62** typically is not used to carry any traffic in the upstream direction and traffic in the downstream direction may be optionally disabled.

The upstream direction is defined as the direction of transmission running from the user to the carrier network. The downstream direction is defined as the direction of transmission running from the carrier network to the user. The provision of a working PVC and a single protection PVC to a user LAN is referred to hereinafter as dual-homing to two COs. The provision of a working PVC and multiple protection PVCs is referred to hereinafter as multi-homing to multiple COs. For simplicity of presentation, the present invention will be described with reference to dual-homing but it is understood that the same principals could be applied to multi-homing.

In accordance with the present invention each CO could be connected to separate router devices in the carrier network or alternatively to the same router device without departing from the spirit of the present invention. Also, each CO could be connected to separate bridged service devices or alternatively to the

same bridged service device without departing from the spirit of the present invention.

B. Failure Detection

The multi-homing system is implemented such that switching from a working PVC **60** to a protection PVC **62** has little or no impact on the user LAN **32**. Figure 7 illustrates a situation where a protection switching has occurred due to a failure of the CO **38**, a failure in the working paths **50, 52**, or a failure of the routed service **44**. At the AC **14**, the traffic is switched to the protection PVC **62**. Upstream and downstream traffic now flows through the protection paths.

1. Backbone Router failure detection

The CC **16** at CO #1 **38** implements a number of failure detection mechanisms to detect IP layer failures with the routed service, which preferably is provided by a BR **5**. If a failure occurs with the BR **5**, the CC at CO #1 **38** can detect the failure using an OSPF failure detection mechanism, a RIP failure detection mechanism, and an active detection mechanism. These detection mechanisms are configurable on a PVC basis in the CC. These failure detection mechanism will be described more fully below.

Upon detection of a BR **5** failure at the other end of the working ATM or FR path **50**, the CC at CO #1 **38** notifies the AC **14** at node **36** that the working PVC **60** is in a faulty condition so that the AC **14** at node **36** can switch traffic to the protection PVC **62**. The CC at CO #1 **38** preferably notifies the AC **14** at node **36** of the failure via an asynchronous virtual path control protocol ("VPCP") message to the AC **14** at node **36**. The VPCP message is a message used on optical ring networks to transfer status information. The VPCP message provides a digital link channel identifier ("DLCI") and status information

regarding the digital channel identified by the DLCI number. The cause of the fault, in this case, is the failure of the BR **5**, and it is not reported by the CC **16** to the AC **14**.

a. OSPF Failure Detection

A first failure detection mechanism for detecting BR **5** failures is an Open Shortest Path Protocol ("OSPF") snooping function that is implemented by the CC **16**. When using this function, the CC **16** inspects incoming OSPF messages on the working FR/ATM path **50**. This mechanism can be activated/deactivated on a per PVC basis. Upon failure to receive a *hello* packet from the BR **5** within a configurable timing window called a *dead timer*, the CC **16** declares a failure of the BR **5**.

If the dead timer expires, the CC **16** preferably determines that the BR **5** is down. The BR **5** sends hello packets at designated intervals which are configurable in the **BR** 5. Therefore, the dead timer preferably should be configurable. Preferably, the default value of the dead timer is four times the value of the Hello interval. That results in a dead timer default of 40 seconds for broadcast networks and two minutes for non-broadcast networks.

The BR **5** can be declared functional and the working path **52** active if three consecutive hellos are received without the timer expiring. The CC **16** can then notify the AC **14** that the PVC **60** is operational via a VPCP message.

b. RIP Failure Detection

A second failure detection mechanism for detecting BR **5** failures is the RIP failure detection mechanism implemented by the CC **16**. When using this failure detection mechanism, the CC **16** can declare the BR **5** down and the PVC not active after a configurable time (preferably more than 30 seconds) during which the CC **16** did not receive any RIP messages from the BR **5**. To reactivate the PVC, the CC **16** can declare the BR **5** up and the PVC active if a number of

consecutive RIP messages are received, preferably three, without the timer expiring. The CC **16** notifies the AC **14** of the status of the PVC via a VPCP message.

c. Active Detection of Router Failure

A third failure detection mechanism available for detecting BR **5** failures is an active detection mechanism. When using this failure detection mechanism, the CC **16** makes use of its IP address. Each CC **16** has a "service entity" with an IP layer address associated with a "service" PVC; several agents can reside at that address such as the DHCP Relay agent. No traffic flows on the service PVC other than traffic that the Service Entity originates. Figure 8 illustrates the active detection mechanism. The service entity residing in the CC **16** uses the "ping" application to verify that the BR **5** is up, using ICMP Echo messages as described in RFC 792 (ICMP), which is incorporated herein by reference. If a number of consecutive pings, preferably more than 3, are unsuccessful (no echo reply), the CC can declare that the BR **5** is unreachable and issue VPCP messages to that effect to the AC **14** for all the working routed VCs terminated to the same Router **5** as the "service PVC." The CC **16** can reactivate the working PVC if more than preferably 3 consecutive pings are successful and will notify the AC **14** via a VPCP message.

2. CC1 Failure

The multi-homing system is capable of switching traffic from the working PVC to the protection PVC in the case of a failure with the CC **1** in the working PVC. In this case, the node that contains CC **2** detects the failure of CC **1** and notifies the AC which in turn switches traffic to the protection PVC as illustrated in Figure 9. CC **2** may be informed of the CC **1** failure by other nodes via a new protocol or via VPCP extensions. When informed, CC **2** then enables the "Add/Drop" cross-connect with backbone router **R2**.

Backbone router **R1**, LAN router LR and the LAN hosts detect dynamically that the link to the working PVC **60** is broken and makes use of normal routing protocols to overcome this failure. For example, backbone router R1 may detect CC1 failure from ATM OAM (AIS/RDI cells, Continuity Check) or from LOS at SONET layer. As the default is declared, the working PVC **60** is declared down and the backbone router R1 link to the customer network is no longer valid. Other backbone routers will be informed of the downed link via routing protocols.

a. CC Failure Detection Mechanism

A failure detection mechanism utilized in the multi-homing system for detecting CC failures is described next. When the CC in CO# 1 **70** fails, the neighbor nodes will detect the failure at SONET level and will trigger the Wrap mechanism illustrated in Figure 10. The AC at node **72** sends traffic to the working path, in this case the "east" path (1). Then, the node next to the node **72** with the failed CC (2) wraps the packs, and sets the FWN bit. The FWN bit is a bit in the SONNET header that indicates whether the frame has been wrapped within the ring. The wrapped packets arrive to the AC at node **72** (3), where they are dropped and continued. Dropped means being taken from the ring traffic and handed off to a local interface. Continued means forwarded to other network nodes. The AC at node **72** performs Path switching and new packets coming from the Customer Network **76** are sent to the "west" path (4). The other neighbor node **78** wraps packets with FWN = 0 and drops packets with FWN=1 (5). Packets addressed to the failed CC then come back to the AC at node **72** from the west path (6). The AC detects the resulting "oscillation" and performs VC switching on the "oscillating" VC, as illustrated in the State machine in Figure 11. The operation of the AC to detect the CC failure is illustrated in figure 11 and the following Tables 1 and 2.

Event	Description
1	FWN signal on working VC, received from the current forwarding Path
2	FWN signal on working VC, received from the new current forwarding Path (after Path switching)
3	Continuity asserted and WTR

Table 1 Events associated with CC failure detection

State	Description
Normal	Normal operating state for the working PVC
Path Switching	Path switching state
CC failure detected	CC failure has been detected in the AC.

Table 2 States associated with CC failure detection

3. Physical and Layer 2 fault detection

The multi-homing system has a mechanism for detecting physical and Layer 2 faults. The CC **16** detects Asynchronous transfer mode ("ATM") layer faults via OAM F4/F5 cells. F4/F5 AIS/RDI faults are preferably detected. The CC **16** responds to received AIS cells by sending RDI cells.

The CC **16** detects frame relay ("FR") layer PVC faults via LMI. When the working PVC becomes unavailable due to a failure at the ATM, FR or SONET level of the CC **16** interface, the CC **16** alerts the AC **14** by sending a

VPCP message. The VPCP messages issued by the CC **16** report the status of the VCs.

C. VC Switching Mechanism

The present invention provides a number of mechanisms for switching traffic from a working PVC **60** to a protection PVC **62**. In a first case, when CC1 **80** detects a backbone router **R1** failure, CC1 **80** configures the PVC **60** with a "continue" cross-connect and passes traffic through to CC2 **82** as illustrated in Figure 12. CC2 is also informed of the failure and it functions as an "add/drop" cross-connect to backbone router **R2**.

CC2 **82** can detect the failure of backbone router **R1** in a number of ways. CC2 **82** can be notified of the failure via VPCP messages when it observes that CC1 **80** is no longer a transmitter for the PVC coming from backbone router **R1**. CC2 **82** can detect the failure when that PVC "expires" as there are no more nodes which put that PVC in the Status Report message. Also, CC2 **82** can be notified of the failure via a new asynchronous message carried by VPCP and sent by the node that contains CC1 **80**. After notification of the failure of backbone router **R1**, the CC2 **82** configures the PVC with an "add/drop" cross-connect with backbone router **R2**.

Switching back to the original PVC can also be enabled. When the backbone router **R1** becomes operational again, the original path may optionally be automatically restored (a.k.a. "revertive switching") if CC1 informs CC2 that the backbone router **R1** is available. Also, in the case of failure with CC2 and/or BR2 failure, the original path may be restored if CC1 informs CC2 that the backbone router **R1** is available.

In a second case, CC1 **80** notifies the AC **84** and CC2 **82**, for example, by means of VPCP or via a wrap mechanism, of the failure. As illustrated in Figure 13, the AC **84** switches traffic to a protection PVC having the same digital link connection identifier "DLCI" number, in the protection path. CC2 **82** enables

"add/drop" cross-connect capability of the protection PVC. CC1 **80** also configures that PVC with a "continue" cross-connect from CC1 **80** to CC2 **82**.

Revertive switching can be enabled by CC1 **80** informing CC2 **82** and AC **84** when the backbone router **R1** is available in case of CC2/BR2 failure.

Third, CC1 **80** notifies the AC **84** and CC2 **82**, for example, by means of VPCP of the failure. As illustrated in Figure 14, the AC **84** switches traffic to a protection PVC having a different DLCI number. CC2 **82** enables "add/drop" cross-connect capability of the protection PVC.

Revertive switching can be enabled by CC1 **80** informing AC **84** when the backbone router **R1** is available in case of CC2/BR2 failure.

Alternatively, BR failure detection can reside in the AC **84**, and the CC simply propagates indications of low level failures of the ATM (POS) to devices on the ring . In this case it is the AC **84** that notifies the CC2 **82** that the working PVC is no longer valid.

1. Switching mechanism description

Upon failure of the working path, the AC **84** is notified by means of VPCP and Wrap mechanism and switches traffic to a protection PVC, with a different DLCI number. The CC2 **82** is configured to drop traffic from the protection VC.

The AC **84** treatment of packets flowing through the working PVC before switching is normal. If the user LAN **86** is connected to a routed VC, devices on the user LAN **86** preferably learn their IP address from the IRDP mechanism. Before VC switching, downstream traffic coming from protection VC is preferably forwarded but optionally could be discarded. The VC switching preferably is configured on a VC basis as revertive but optionally could be configured as non-revertive.

The state machine shown in Figure 15 illustrates a preferred revertive switching process. The state machine shown in Figure 16 illustrates a preferred

non-revertive switching process. The events that trigger state transitions are listed below in Table 3 in order of descending priority, from 1 to 7. If more than one event occurs at a given time, the state transition shall be triggered by the event with highest priority, in accordance with Table 3. The various states are described below in Table 4.

Event	Description
1	Lockout of Protection
2	CC failure condition
3	Protection VC failure
4	Forced switch for working VC
5	Working VC failure
6	Manual switch for working VC
7	Manual switch for protection VC
8	No request of switch[1]

Table 3 Events description for VC switching

State	Description
Working	Upstream traffic is transmitted to working VC, and downstream traffic is forwarded according to the parameter *Enable downstream traffic from protection VC*
Protection	Upstream traffic is transmitted to protection VC, and downstream traffic is forwarded according to the parameter *Enable downstream traffic from protection VC*
Wait to restore	Upstream and downstream traffic flows through protection VC. WTR timer is configurable
Do not Revert	Upstream traffic is transmitted to protection VC, and downstream traffic is forwarded according to the parameter *Enable downstream traffic from protection VC*

[1] This event means "there are no events", that is none of 1-6 event.

Table 4 States description for VC switching

The AC 84 can issue the following commands: Lockout of Protection, Forced switch for working VC, Manual switch for protection VC, and manual switch for working VC. The Lockout of Protection command denies all working traffic access to the protection entity. The Forced switch for working VC command switches traffic to the protection VC unless the protection VC is in a faulty condition. The Manual switch for protection VC command switches traffic from protection VC to working VC. Finally, the Manual switch for working VC command switches traffic from working VC to protection VC.

After VC switching, every entity associated to the working VC (such as MAC address, the ARP process and cache, the RIP and IRDP learning processes and DHCP Relay agent) is associated to the protection routed VC. Downstream routed traffic is restored as soon as the Router at CO#2 discovers the topology change and that the LAN can now be reached via protection VC. Bridged service is restored as soon as the PVC is switched. After VC switching IRDP traffic coming from the router shall be snooped, and IP address auto-configuration will assign the IP address to the protection routed VC. If the IP address is different to that of the working VC, a gratuitous ARP shall be sent with the new IP address and the MAC address of the Ethernet Port.

2. Configurable parameters

A number of parameters are configurable. The wait to restore ("WTR") timer is preferably set to 60 seconds and preferably has a range of acceptable values from 1-300 seconds.

In the preferred system, the following parameters are configurable in the AC per PVC: (1) VC switching enabled (ON/OFF*); (2) Revertive VC switching(ON/OFF*); (3) DLCI of protection VC (valid DLCI number); and (4)

Enable downstream traffic from protection VC (ON*/OFF). The states followed by the asterisk are the default states in the preferred system

In the preferred system, the following parameters are configurable in the CC per PVC: (1) ATM layer failure detection enabled (ON/OFF*); (2) IP layer OSPF failure detection enabled (ON/OFF*); (3) OSPF Dead timer (1-255 seconds); (4) IP layer RIP failure detection (ON/OFF*); (5) RIP timer (30-300 seconds, default 75); (6) Ping mechanism enable (ON/OFF*); and (7) Ping interval (1-60 seconds, default 10).

D. Impact on Customer Network Configurations

1. Bridged VC

The protection system of the present invention can be utilized in a network that uses the common carrier to provide a bridged connection for data traffic from a user network **96** to a remote network **98**. Such a network could be have an asymmetric topology or a symmetric topology.

a. Asymmetric Configuration

An exemplary asymmetric configuration is shown in figure 17 in which there is a ring network **90** on one end of the carrier network **92** and a L2 switch **94** at the other end. The carrier **92** bridges the traffic from the customer network **96** to a remote location **98**, presenting two Ethernet bridged ATM PVCs **91, 93** to the remote network **98**. Preferably, the remote network **98** interfaces the carrier **92** with a L2 switch **94**, which terminates the ATM signals and extracts Ethernet frames. An exemplary L2 switch **94** is a Catalyst 5000. Alternatively, the L2 switch **94** can be a part of the carrier **92** and the carrier **92** presents a single PVC or Ethernet interface to the remote network **98**.

Before any VC switching, all the traffic passes through the working PVC **91**. The L2 switch **94** is working and passing traffic received through the port **95** connected to the working PVC **91**, but the port **97** connected to the protection PVC does not receive traffic and no MAC addresses are learned by that port **97**. If the ATM switches **99** runs the Spanning Tree Protocol, the bridged port **97** of L2 switch **94** remains in the "block state": it does not participate in frame relay and discards received frames. The bridge, however, includes the port **97** in the computation of the active topology.

After VC switching due to a detected failure, the switch **94** will receive frames coming from the protection PVC **93**, and the port **97** will learn MAC addresses on the remote network **98**. The switch **94** forwards frames received from the port **97** that is connected to the protection PVC **93**. The primary impact to the hosts and routers on the customer networks **96, 98** due to VC switching is that the devices on the customer networks **96, 98** must learn their new IP addresses using traditional protocols after VC switching occurs.

b. Symmetric Configuration

An exemplary symmetric configuration network is shown in figure 18 in which there is a ring network **100** on each end of the carrier network **102**. Each AC **104** sends bridged traffic to to the far end AC **104** using the working VC **106**. Each AC **104** forwards downstream traffic coming from both protection **108** and working **108** VCs.

When a fault occurs in the ATM network **102**, the fault will be reported to both the ACs **104** via ATM OAM cells (AIS/RDI) or Frame Relay LMI and VPCP. As a result, The two ACs **104** will switch forwarding of traffic to the protection PVC **108**. The primary impact to the hosts and routers on the customer networks **109** due to VC switching is that the devices on the customer

networks **109** must learn their new IP addresses using traditional protocols after VC switching occurs.

2. Routed VC

In the case of routed VCs, the impact of VC switching on customer networks is minimal. An exemplary system is illustrated in figure 19. Backbone router 1 **110** is connected to the LAN **112** via the working end to end PVC **114**. Backbone router 2 **116** is operational and connected to the backbone of the carrier network. The backbone router 2 **116** interface is configured as if attached to the customer LAN **112**. An ATM/FR PVC **117** is configured and terminated in the CC #2 **119** and is inter-worked with the protection VC **121** inside the ring **118**. To minimize the impact on the customer network, the IP address of the backbone router 2 **116** interface is preferably the same as the IP address of the backbone router 1 **110** interface as illustrated in figure 20. Traffic passes through CC #1 **120**. The AC **122** treatment of packets to/from the working PVC **114** is normal. If the customer port is connected to a routed VC, it may learn its IP address from IRDP. Backbone router 2 **116** cannot reach the LAN router **123** and cannot establish adjacency with it.

After VC switching Backbone router 1 **110**, LAN router **123** and the hosts **124** detect dynamically that the working PVC **114** is broken and recover from this situation through the routing protocols. When there is a failure of CC #1 **120** or of the working ATM/FR PVC, the OAM cells or the LMI will notify the Backbone router 1 **110** and it will declare the ATM/FR sub-interface as down. The routing protocols will take appropriate action, and after a re-convergence period of time, the other routers will learn the new topology and send traffic via the backbone router 2 **116** . Similarly, the LAN router **123** will learn the new topology because of its routing protocol.

a. Flat customer LAN

Hosts **124** attached to the LAN **112** should detect the failure of Backbone router 1 **110** and react dynamically to recover from the situation. There are several options for the configuration and behavior of the hosts **124**. In one embodiment, the hosts **124** on the LAN **112** have configured a default gateway. Using this method a host **124** is statically configured to know the IP address of its default router. If that router, however, becomes unavailable, the host **124** will not be able to communicate with devices off of the local LAN segment **112** even if there is another router available through an alternative PVC. In this embodiment, the hosts **124** must be manually re-configured so that the backbone can be reachable.

In a second embodiment, the hosts **124** on the LAN **112** are configured with a list of default gateways. If the primary default gateway fails, the hosts **124** detect the failure and switch automatically to the next default gateway in the list. The default gateway list preferably includes Backbone router 1 **110** and Backbone router 2 **116** . VC switching preferably occurs before hosts **124** begin sending packets to Backbone router 2 **116** so that disruption of upstream service is minimized. In this embodiment, the hosts **124**, the hosts **124** automatically reconfigure themselves as soon as they learn by IRDP or RIP that Backbone router 2 **116** is available.

In a third embodiment, the hosts **124** on the LAN **112** use the ICMP Router Discover Protocol ("IRDP") to listen to router hellos. This allows a host **124** to quickly adapt to changes in network topology. IRDP may help hosts **124** to update their route cache and default gateway list. To facilitate this, after VC switching has occurred, Backbone router 2 **116** preferably transmits unsolicited IRDP advertisements. As a result, the hosts **124** can readily add cache and default gateway list. To facilitate this, after VC switching has occurred, Backbone to their list of default gateways. In this embodiment, the hosts **124**, the

hosts **124** automatically reconfigure themselves as soon as they learn by IRDP that Backbone router 2 **116** is available.

In a fourth embodiment, IP hosts **124** use "silent RIP" to 'learn' the available upstream gateways and builds their own default router tables. In this embodiment, the hosts **124**, the hosts **124** automatically reconfigure themselves as soon as they learn by RIP that Backbone router 2 **116** is available.

To minimize the period of service disruption and operational complexity, The backbone routers may optionally be provisioned with the same IP address on the customer LAN **112**, as illustrated in Figure 20.

b. Customer network with firewall

Illustrated in figure 21 is a customer network that utilizes a firewall **130**. The network between the firewall and the WAN link is usually referred to as Demilitarized zone **132** ("DMZ"). Bastion hosts **134**, such as the WWW server and the mail server, preferably are also coupled to the DMZ **134**. The firewall **130** is configured with a default gateway for the upstream traffic. In case of failure of the path to backbone router R1 **136**, VC switching mechanisms intervenes and the upstream gateway for the firewall changes.

In an alternative embodiment, as shown in figure 22, a router **140** is coupled between the DMZ **132** and the ring **142**. This configuration is often called "screened subnet". This case is similar to the configuration with a LAN and a single Router connected to the AC.

Having described in detail the preferred embodiments of the present invention, including preferred modes of operation, it is to be understood that this invention and operation could be constructed and carried out with different elements and steps. The preferred embodiments are presented only by way of example and are not meant to limit the scope of the present invention, which is defined by the following claims.

What is claimed:

1. A system for providing a customer network with high speed access to a carrier network, the system comprising:

an access device for providing a communication path for the customer network, said access device being operable to receive data traffic from the customer network and to forward the data traffic within the system, the access device also be operable to receive data traffic from the system and to drop some of the data traffic to the customer network;

a first concentrator device in communication with the access device within the system, said first concentrator device being operable to establish a communication path with the carrier network, said first concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic; and

a second concentrator device in communication with the access device and the first concentrator device within the system, said second concentrator device being operable to establish a communication path with the carrier network, said second concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic;

wherein the access device and the first concentrator device cooperate to form a first virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the first virtual channel is the primary communication channel for the customer network;

wherein the access device and the second concentrator device cooperate to form a second virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer

network and wherein the second virtual channel is a backup communication channel for the customer network; and

wherein the system is operable to switch the primary communication channel from the first virtual channel to the second virtual channel upon detection of a failure in the first virtual channel.

2. The system according to claim 1 wherein the first concentrator device establishes a communication path with the carrier network by establishing a communication path with one or more routers or bridges in the carrier network and the second concentrator device established a communication path with the carrier network by establishing a communication path with one or more routers or bridges in the carrier network.

3. The system according to claim 1 wherein the first concentrator device is operable to execute a failure detection mechanism that is capable of detecings router failures and operable to communicate to the access device that the first virtual channel is not functioning upon the detection of a router failure.

4. The system according to claim 3 wherein the failure detection mechanism makes use of an Open Shortest Path Protocol.

5. The system according to claim 3 wherein the failure detection mechanism makes use of a routing internet protocol.

6. The system according to claim 3 wherein the failure detection mechanism makes use of a ping application.

7. The system according to claim 1 wherein the second concentrator device is operable to detect a failed condition with the first concentrator device and to notify the access device of the failure.

8. The system according to claim 1 wherein the access device is operable to detect a failed condition with the first concentrator device by detecting packet oscillation in the system.

9. The system according to claim 1 wherein the access device is operable to cause the primary communication channel to switch from the first virtual

channel to the second virtual channel when one or more of the follow events are detected: a failure of the first concentrator device is detected, the access device is commanded to cause the switch, a failure of the communication path between the first concentrator device and the carrier network is detected, a failure of a backbone router coupled to the first concentrator device is detected, or a failure of a bridge device coupled to the first concentrator device is detected.

10. The system according to claim 1 wherein the access device is operable to cause the primary communication channel to switch from the second virtual channel to the first virtual channel when one or more of the follow events are detected: the first concentrator device has recovered from a failure, a recovery of the communication path between the first concentrator device and the carrier network is detected, a failure of the second concentrator device is detected, the access device is commanded to cause the switch, a failure of the communication path between the second concentrator device and the carrier network is detected, a failure of a backbone router coupled to the second concentrator device is detected, or a failure of a bridge device coupled to the second concentrator device is detected.

11. The system according to claim 1 wherein the system comprises a plurality of network nodes and wherein the access device, the first concentrator device and the second concentrator device are each located at different network nodes.

12. The system according to claim 1 wherein the system comprises a plurality of network nodes and wherein the access device and one of said first concentrator device and said second concentrator device are located at the same network node.

13. An access device for use in a network node apparatus in a system comprising (a) a first concentrator device that is operable to communicate with the access device, said first concentrator device being operable to establish a communication path with a carrier network, said first concentrator device being

operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic, and (b) a second concentrator device that is operable to communicate with the access device and the first concentrator device, said second concentrator device being operable to establish a communication path with the carrier network, said second concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic, wherein the access device and the first concentrator device are operable to cooperate to form a first virtual channel for allowing data traffic to flow from a customer network to the carrier network and from the carrier network to the customer network and wherein the first virtual channel is the primary communication channel for the customer network, and wherein the access device and the second concentrator device are operable to cooperate to form a second virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the second virtual channel is a backup communication channel for the customer network, the access device being operable to effect the following steps:

detecting an failure in the first virtual channel; and

switching the primary communication channel from the first virtual channel to the second virtual channel.

14. A network system, comprising:

a first node element that is coupled to at least one other network node element, said first node element being operable to receive data from an other having an access interface

a second node element having a concentrator interface

a third node element having a concentrator interface

15. A method for switching a communication channel from a first virtual channel to a second virtual channel in a system comprising (a) an access device

for providing a communication path for a customer network, said access device being operable to receive data traffic from the customer network and to forward the data traffic within the system, the access device also be operable to receive data traffic from the system and to drop some of the data traffic to the customer network, (b) a first concentrator device in communication with the access device within the system, said first concentrator device being operable to establish a communication path with a carrier network, said first concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic, and (c) a second concentrator device in communication with the access device and the first concentrator device within the system, said second concentrator device being operable to establish a communication path with the carrier network, said second concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic, wherein the access device and the first concentrator device cooperate to form the first virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the first virtual channel is the primary communication channel for the customer network, wherein the access device and the second concentrator device cooperate to form the second virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the second virtual channel is a backup communication channel for the customer network, said method comprising the steps of:

detecting a failure in the first virtual channel; and

switching the primary communication channel from the first virtual channel to the second virtual channel.

16. The method according to claim 15 wherein the detecting step comprises the steps of:

detecting a failure in a communication path between the first concentrator device and the carrier network; and

reporting the failure in the communication path between the first concentrator device and the carrier network to the access device.

17. The method according to claim 16 wherein the access device causes the communication channel to switch from the first virtual channel to the second virtual channel in response to receiving a report of the failure.

18. The method according to claim 16 wherein the first concentrator device reports the failure to the access device.

19. The method according to claim 15 wherein the detecting step comprises the steps of detecting a failure in the first concentrator device.

20. The method according to claim 19 wherein the second concentrator device reports the failure to the access device.

21. The method according to claim 19 wherein the access device is operable to detect the failure by detecting packet oscillation in the system.

22. A system for providing a providing a working path and a protection path comprising the steps of:

providing an access device for providing a communication path for a customer network, said access device being operable to receive data traffic from the customer network and to forward the data traffic within the system, the access device also be operable to receive data traffic from the system and to drop some of the data traffic to the customer network;

providing a first concentrator device in communication with the access device within the system, said first concentrator device being operable to establish a communication path with the carrier network, said first concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic;

providing a second concentrator device in communication with the access device and the first concentrator device within the system, said second concentrator device being operable to establish a communication path with the carrier network, said second concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic;

providing a first virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network via the access device and the first concentrator device and wherein the first virtual channel is the primary communication channel for the customer network;

providing a second virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network via the access device and the second concentrator device and wherein the second virtual channel is a backup communication channel for the customer network;

detecting a failure associated with the first virtual channel;

reporting the failure to the access device; and

causing the primary communication channel to switch from the first virtual channel to the second virtual channel in response to the failure.

23. The system according to claim 22 wherein the first concentrator device is operable to detect a failure with a router in the carrier network using an Open Shortest Path Protocol and to report the failure to the access device wherein the access device causes the primary communication channel to switch from the first virtual channel to the second virtual channel in response to notification of the failure.

24. The system according to claim 22 wherein the first concentrator device is operable to detect a failure with a router in the carrier network using a routing internet protocol and to report the failure to the access device wherein the

access device causes the primary communication channel to switch from the first virtual channel to the second virtual channel in response to notification of the failure.

25. The system according to claim 22 wherein the first concentrator device is operable to detect a failure with a router in the carrier network using a ping application and to report the failure to the access device wherein the access device causes the primary communication channel to switch from the first virtual channel to the second virtual channel in response to notification of the failure.

26. The system according to claim 22 wherein the second concentrator device is operable to detect a failure with the first concentrator device and to report the failure to the access device wherein the access device causes the primary communication channel to switch from the first virtual channel to the second virtual channel in response to notification of the failure.

27. The system according to claim 22 wherein the access device is operable to detect a failure with the first concentrator device by detecting packet oscillation in the system and to cause the primary communication channel to switch from the first virtual channel to the second virtual channel in response to detecting the failure.

28. The system according to claim 22 wherein the first concentrator device is operable to detect an asynchronous transfer mode fault in the communication path between the first concentrator device and the carrier network and to report the failure to the access device wherein the access device causes the primary communication channel to switch from the first virtual channel to the second virtual channel in response to notification of the failure.

29. The system according to claim 22 further comprising the steps of:

detecting that the first virtual channel has recovered from a failure state;

reporting the recovery to the access device; and

causing the primary communication channel to switch from the second virtual channel to the first virtual channel in response to detecting the recovery.

30. A medium for storing a computer-executable program, for use with a system comprising (a) an access device for providing a communication path for a customer network, said access device being operable to receive data traffic from the customer network and to forward the data traffic within the system, the access device also be operable to receive data traffic from the system and to drop some of the data traffic to the customer network, (b) a first concentrator device in communication with the access device within the system, said first concentrator device being operable to establish a communication path with the carrier network, said first concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic, (c) a second concentrator device in communication with the access device and the first concentrator device within the system, said second concentrator device being operable to establish a communication path with the carrier network, said second concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic, (d) a first virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network via the access device and the first concentrator device and wherein the first virtual channel is the primary communication channel for the customer network, and (e) a second virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network via the access device and the second concentrator device and wherein the second virtual channel is a backup communication channel for the customer network, the computer executable program effecting a process comprising the steps of:

causing the primary communication channel to switch from the first virtual channel to the second virtual channel in response to the detection of a failure associated with the first virtual channel; and

causing the primary communication channel to switch from the second virtual channel to the first virtual channel in response to the detection of a recovery associated with the first virtual channel.

31. An optical ring network system for providing a customer network with high speed access to a carrier network, the system comprising:

an access device for providing a communication path for the customer network, said access device being operable to receive data traffic from the customer network and to forward the data traffic within the system, the access device also be operable to receive data traffic from the system and to drop some of the data traffic to the customer network;

a first concentrator device in communication with the access device within the system, said first concentrator device being operable to establish a communication path with the carrier network, said first concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic; and

a second concentrator device in communication with the access device and the first concentrator device within the system, said second concentrator device being operable to establish a communication path with the carrier network, said second concentrator device being operable to drop data received from the system to the carrier network and also operable to add data received from the carrier network to the system data traffic;

wherein the access device and the first concentrator device cooperate to form a first virtual channel for allowing data traffic to flow from the customer network to the carrier network and from the carrier network to the customer network and wherein the first virtual channel is the primary communication channel for the customer network;

wherein the access device and the second concentrator device cooperate to form a second virtual channel for allowing data traffic to flow from the customer

network to the carrier network and from the carrier network to the customer network and wherein the second virtual channel is a backup communication channel for the customer network; and

wherein the system is operable to switch the primary communication channel from the first virtual channel to the second virtual channel upon detection of a failure in the first virtual channel.

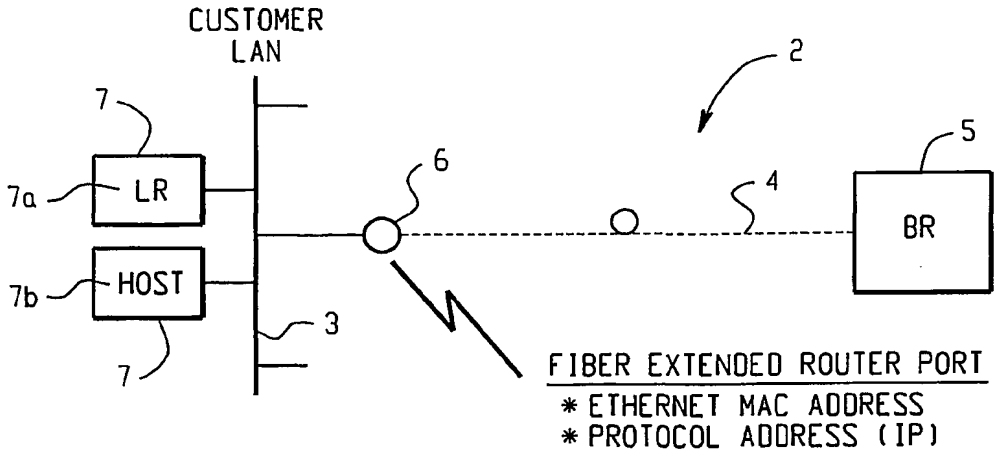

CUSTOMER LAN
7
7a
LR
7b
HOST
7
3
6
2
4
5
BR
FIBER EXTENDED ROUTER PORT
* ETHERNET MAC ADDRESS
* PROTOCOL ADDRESS (IP)

Fig. 1

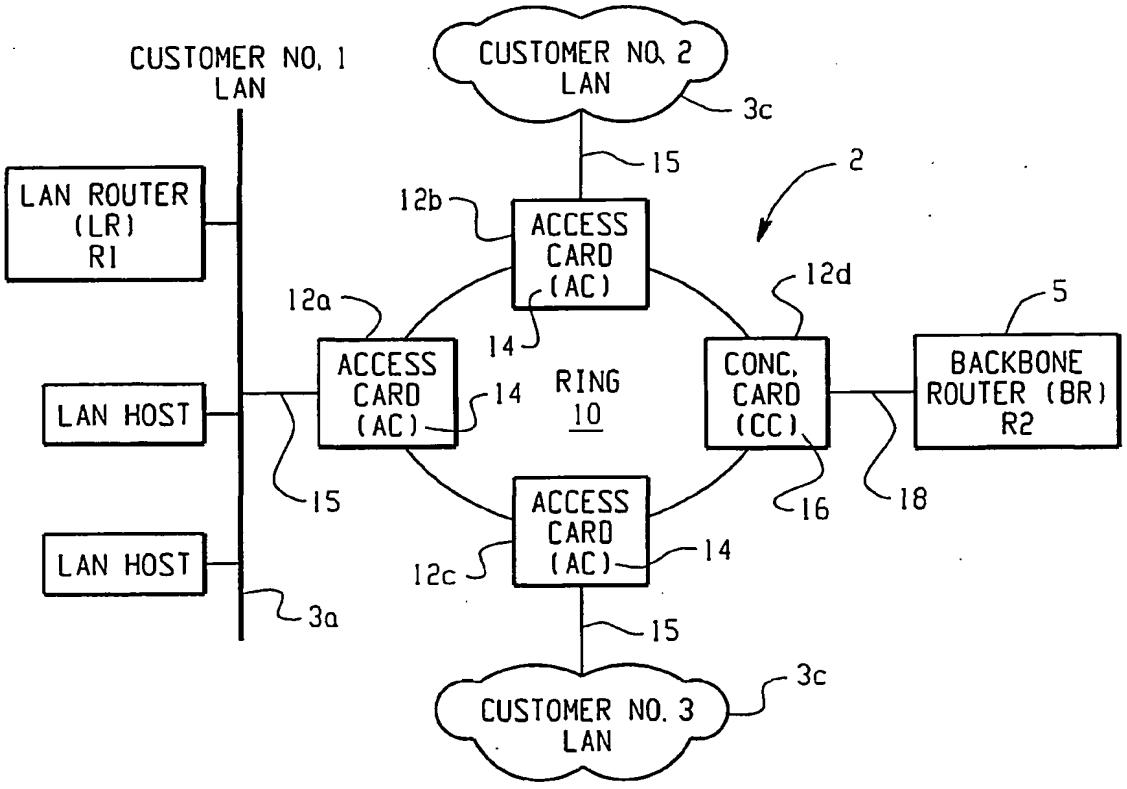

CUSTOMER NO. 1 LAN
CUSTOMER NO. 2 LAN
3c
15
2
LAN ROUTER (LR) R1
12b
ACCESS CARD (AC)
12a
12d
5
14
ACCESS CARD (AC)
14
RING 10
CONC. CARD (CC)
BACKBONE ROUTER (BR) R2
LAN HOST
15
16
18
LAN HOST
ACCESS CARD (AC)
12c
14
3a
15
CUSTOMER NO. 3 LAN
3c

Fig. 2

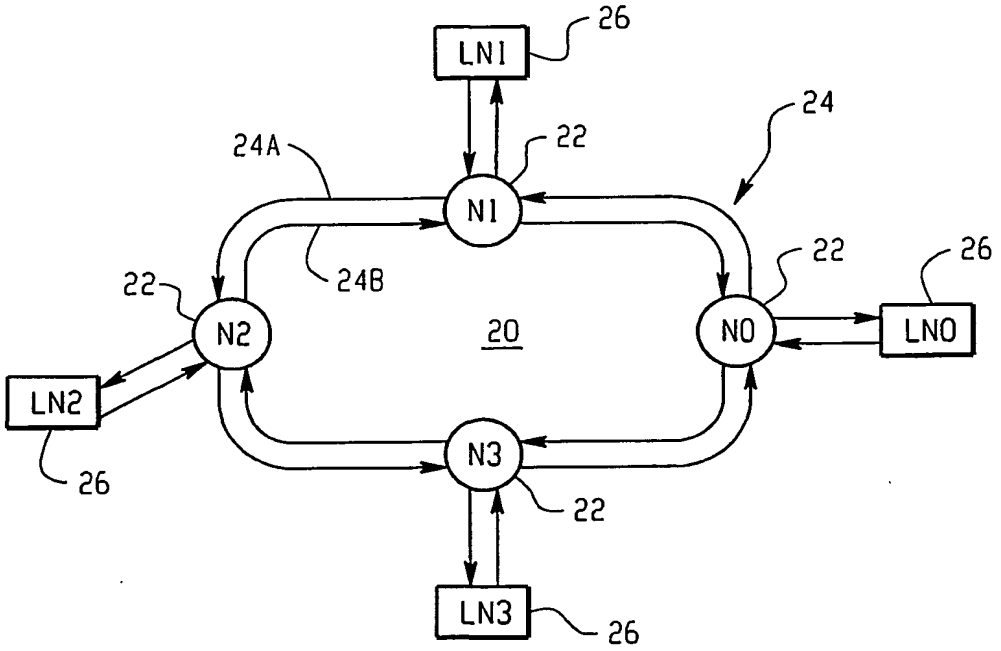

LN1
26
24
24A
22
N1
24B
22
26
22
N2
20
NO
LNO
LN2
26
N3
22
LN3
26

Fig. 3

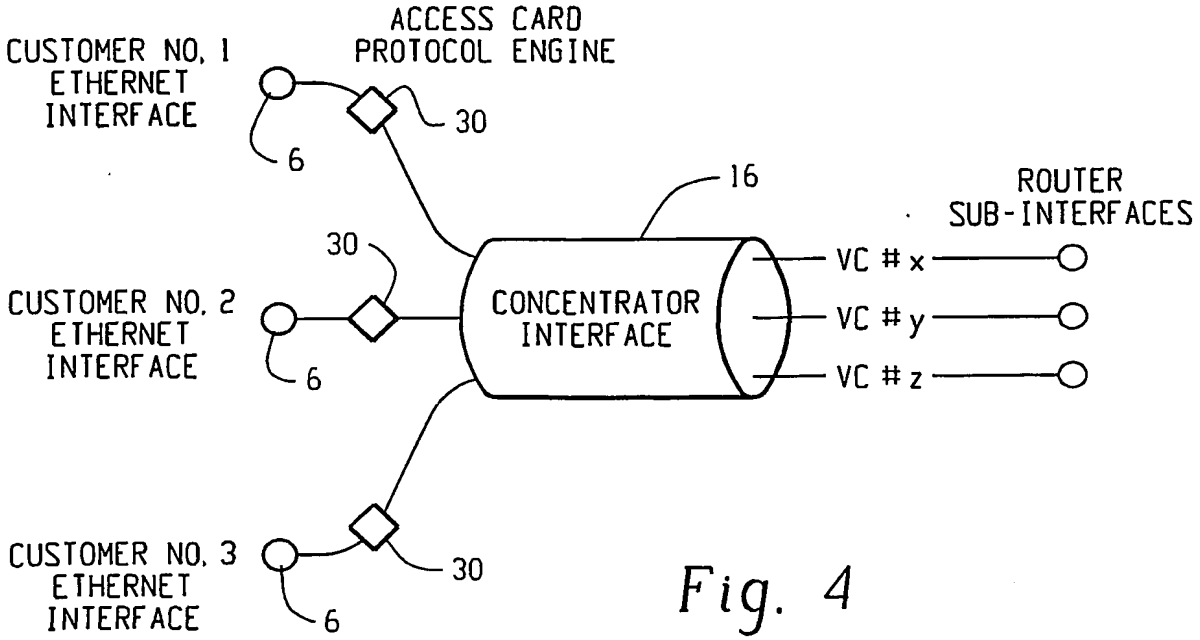

CUSTOMER NO. 1 ETHERNET INTERFACE
ACCESS CARD PROTOCOL ENGINE
30
6
16
ROUTER SUB-INTERFACES
30
CUSTOMER NO. 2 ETHERNET INTERFACE
CONCENTRATOR INTERFACE
VC # x
VC # y
VC # z
6
CUSTOMER NO. 3 ETHERNET INTERFACE
30
6

Fig. 4

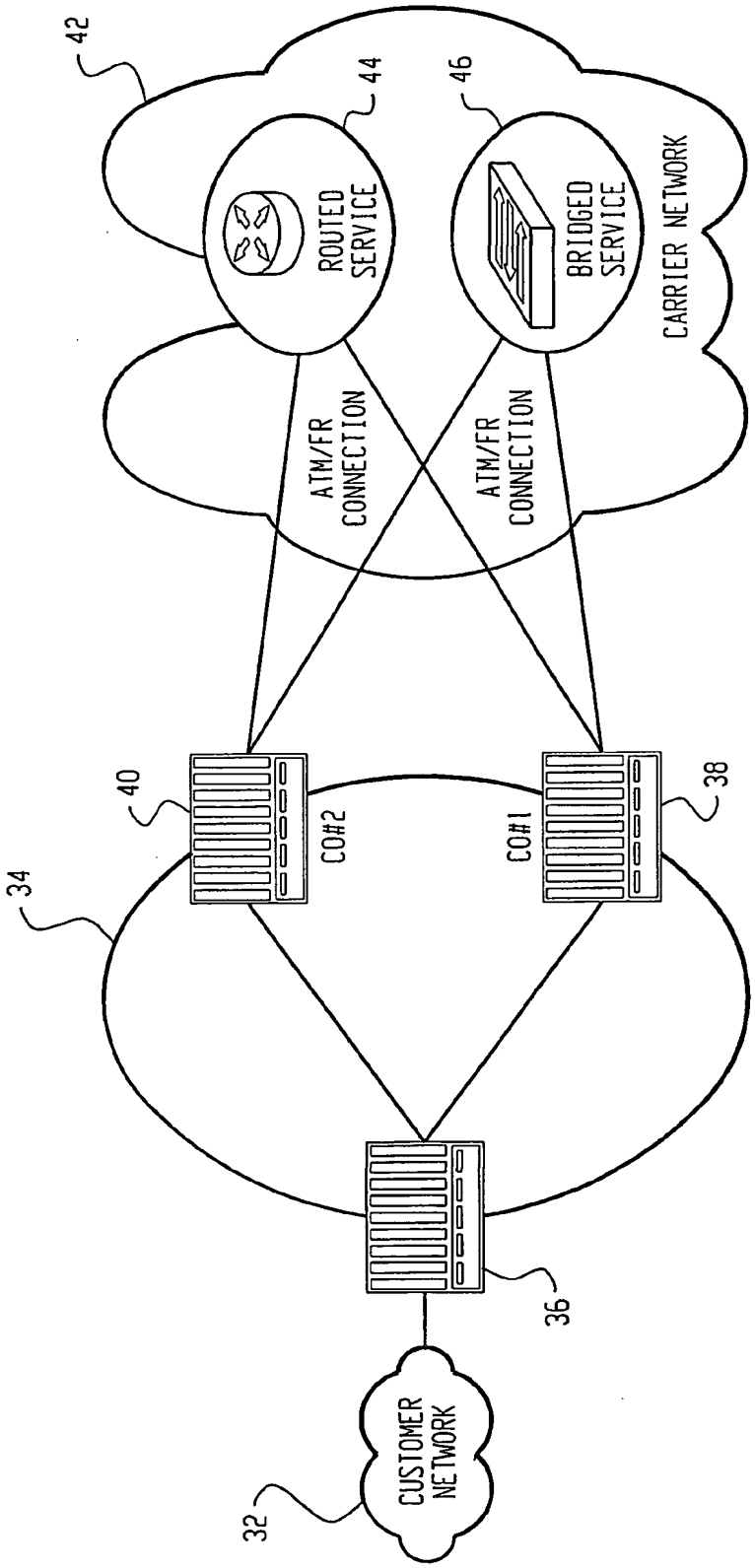

42
44
46
ROUTED SERVICE
BRIDGED SERVICE
CARRIER NETWORK
ATM/FR CONNECTION
ATM/FR CONNECTION
40
CO#2
CO#1
38
34
36
CUSTOMER NETWORK
32

Fig. 5

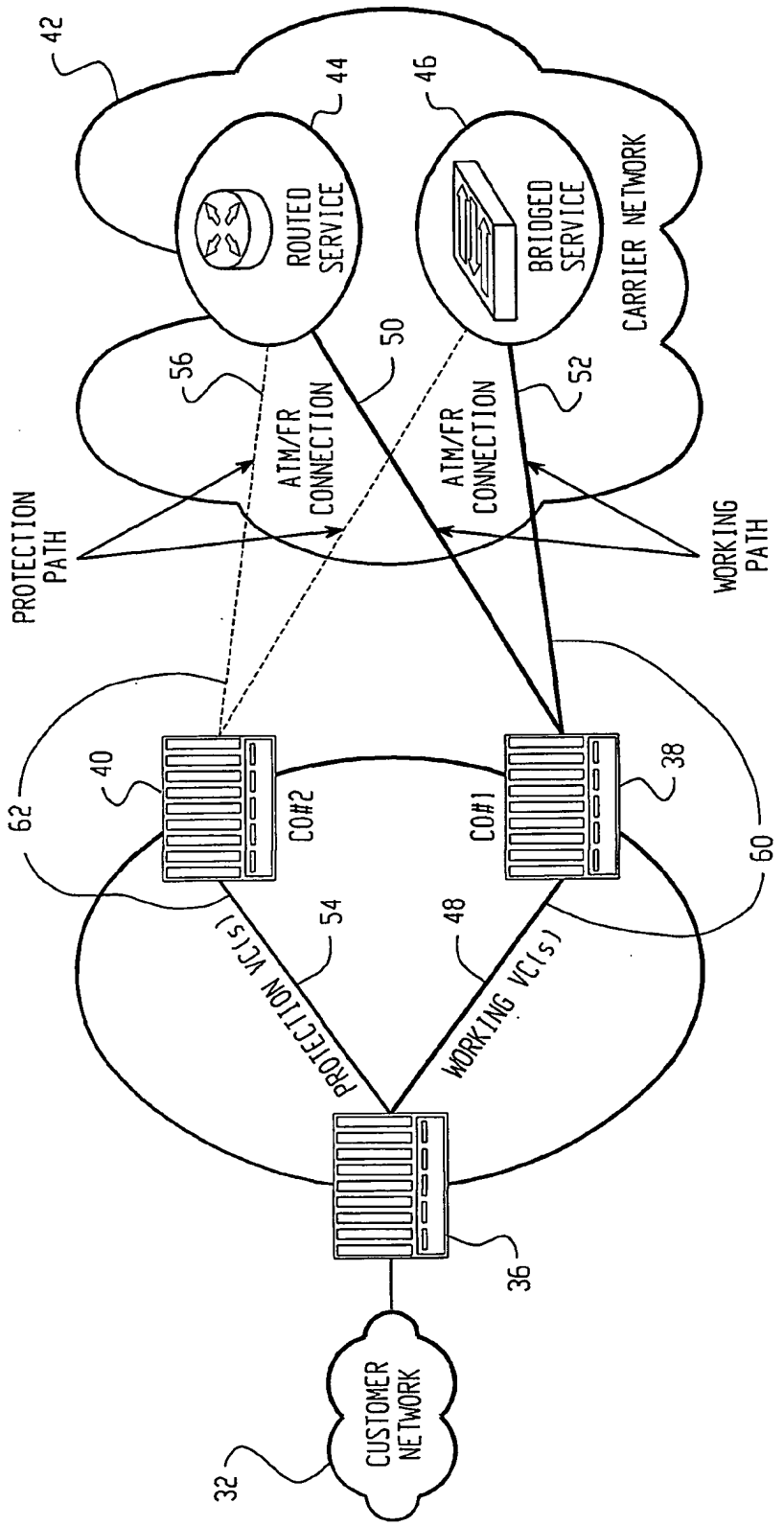

42
44
46
ROUTED SERVICE
BRIDGED SERVICE
CARRIER NETWORK
56
50
52
ATM/FR CONNECTION
ATM/FR CONNECTION
PROTECTION PATH
WORKING PATH
62
40
CO#2
CO#1
38
60
54
48
PROTECTION VC(S)
WORKING VC(S)
36
CUSTOMER NETWORK
32

Fig. 6

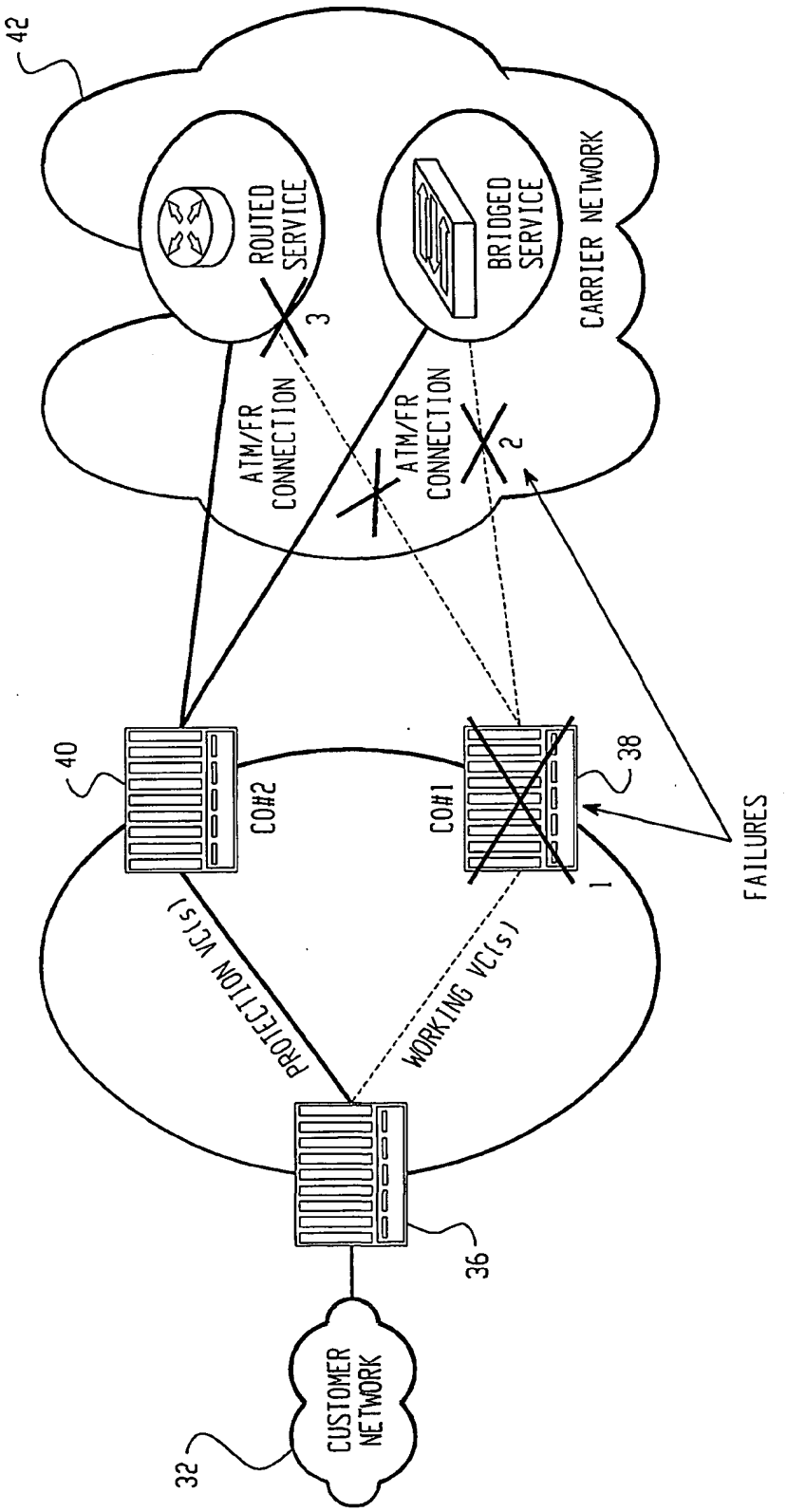

42
ROUTED SERVICE
BRIDGED SERVICE
CARRIER NETWORK
3
ATM/FR CONNECTION
ATM/FR CONNECTION
2
40
CO#2
CO#1
38
1
FAILURES
PROTECTION VC(S)
WORKING VC(S)
36
CUSTOMER NETWORK
32

Fig. 7

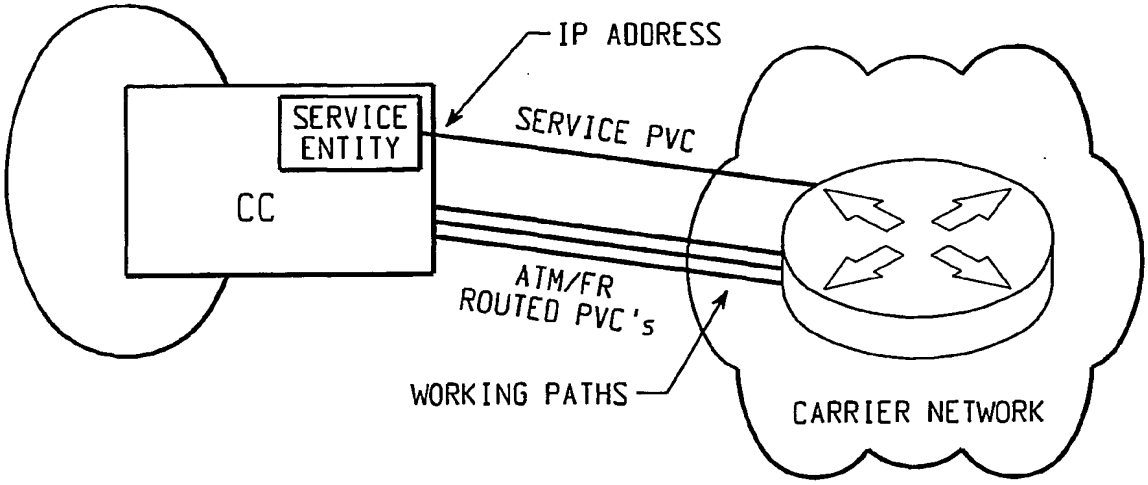

IP ADDRESS
SERVICE ENTITY
SERVICE PVC
CC
ATM/FR ROUTED PVC's
WORKING PATHS
CARRIER NETWORK

Fig. 8

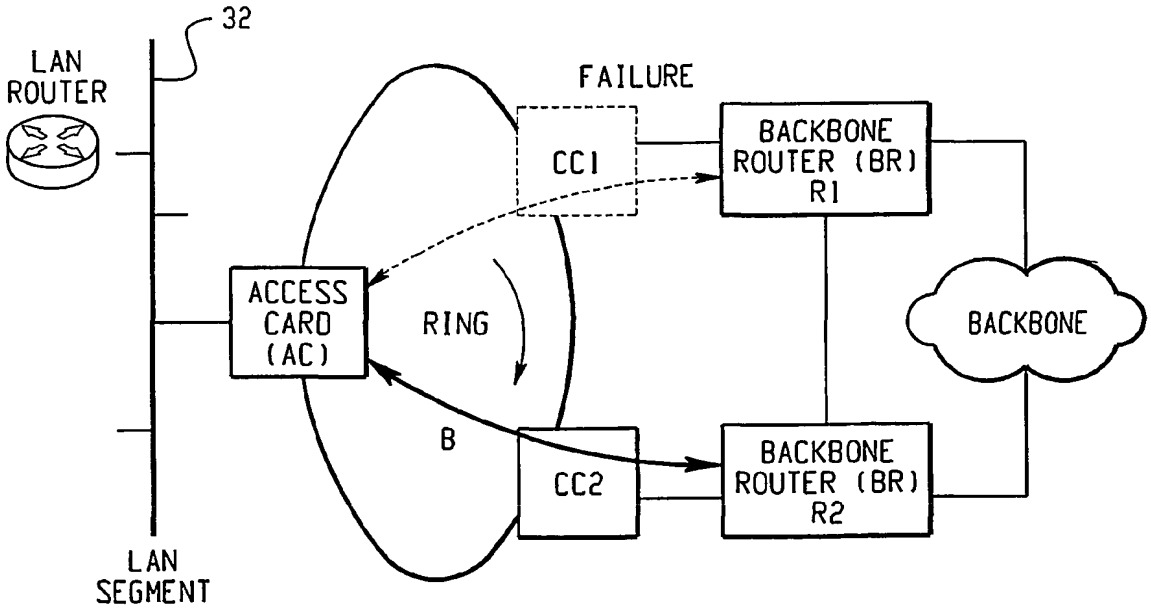

32
LAN ROUTER
FAILURE
CC1
BACKBONE ROUTER (BR) R1
ACCESS CARD (AC)
RING
BACKBONE
B
CC2
BACKBONE ROUTER (BR) R2
LAN SEGMENT

Fig. 9

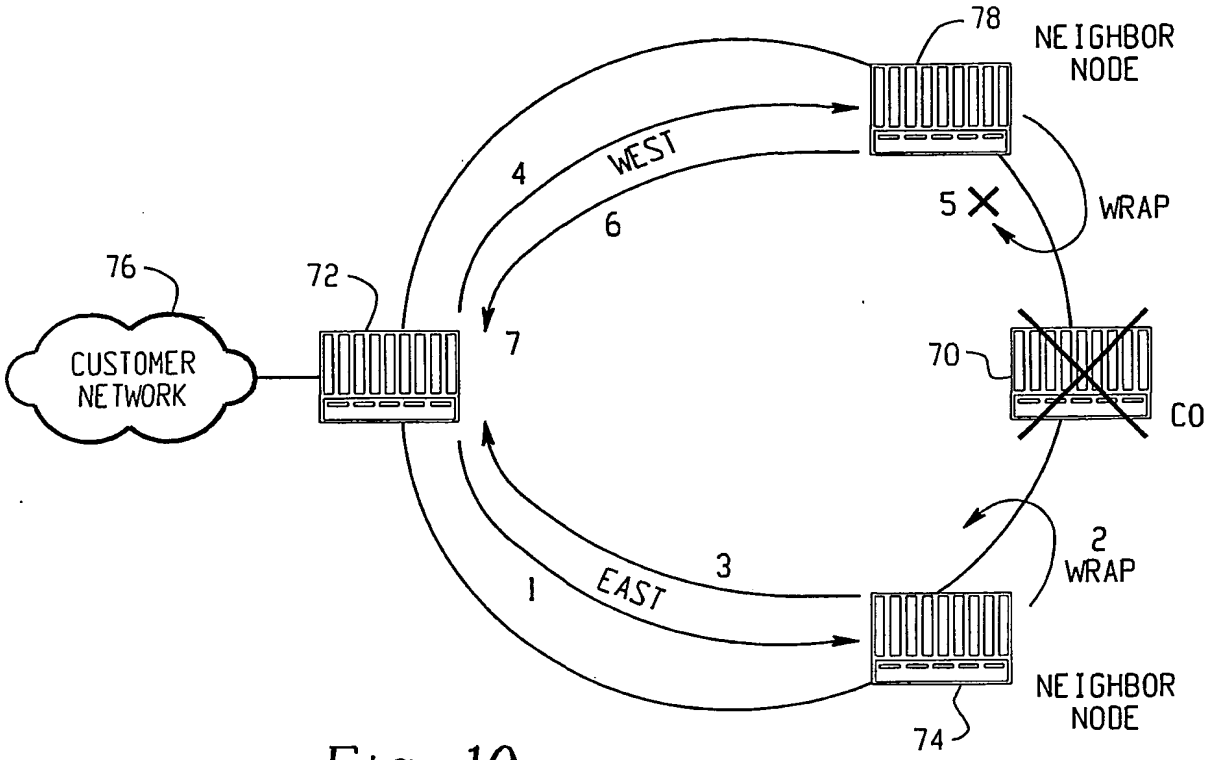

78
NEIGHBOR NODE
4
WEST
6
5
WRAP
76
72
CUSTOMER NETWORK
7
70
CO
2
WRAP
3
1
EAST
NEIGHBOR NODE
74

Fig. 10

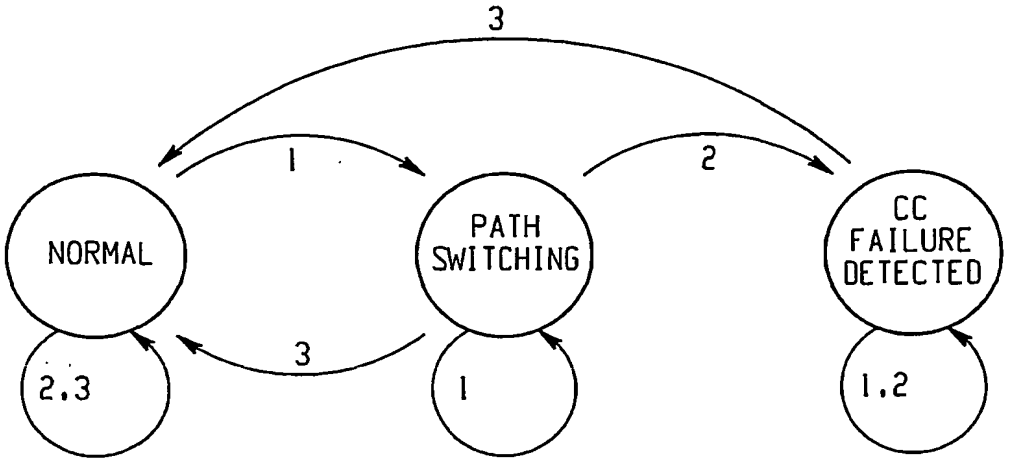

3
1
2
NORMAL
PATH SWITCHING
CC FAILURE DETECTED
3
2,3
1
1,2

Fig. 11

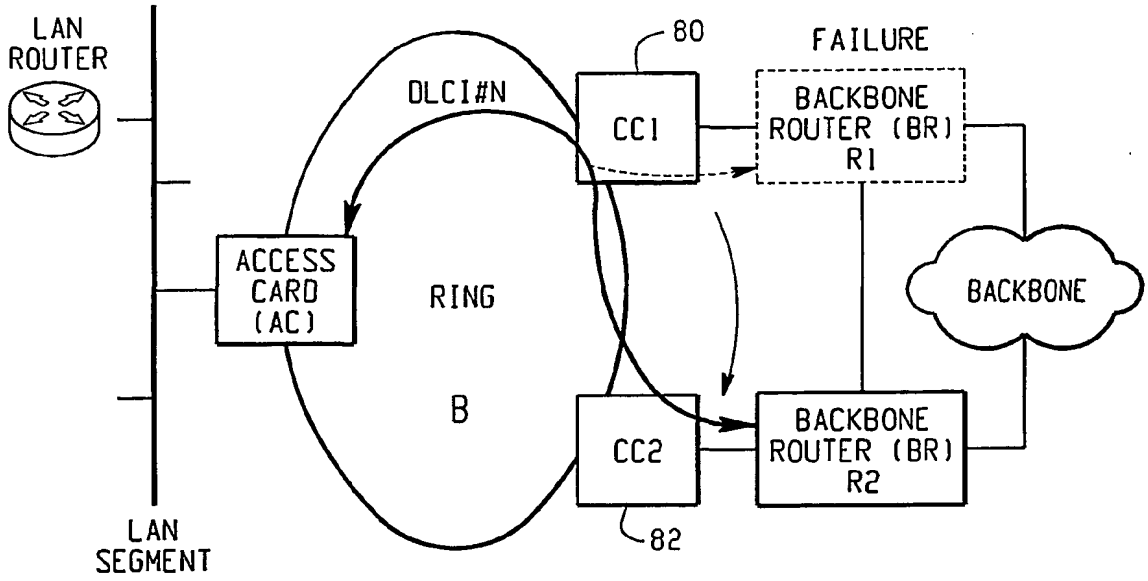

LAN
ROUTER
80
FAILURE
DLCI#N
CC1
BACKBONE
ROUTER (BR)
R1
ACCESS
CARD
(AC)
RING
B
BACKBONE
CC2
BACKBONE
ROUTER (BR)
R2
82
LAN
SEGMENT

Fig. 12

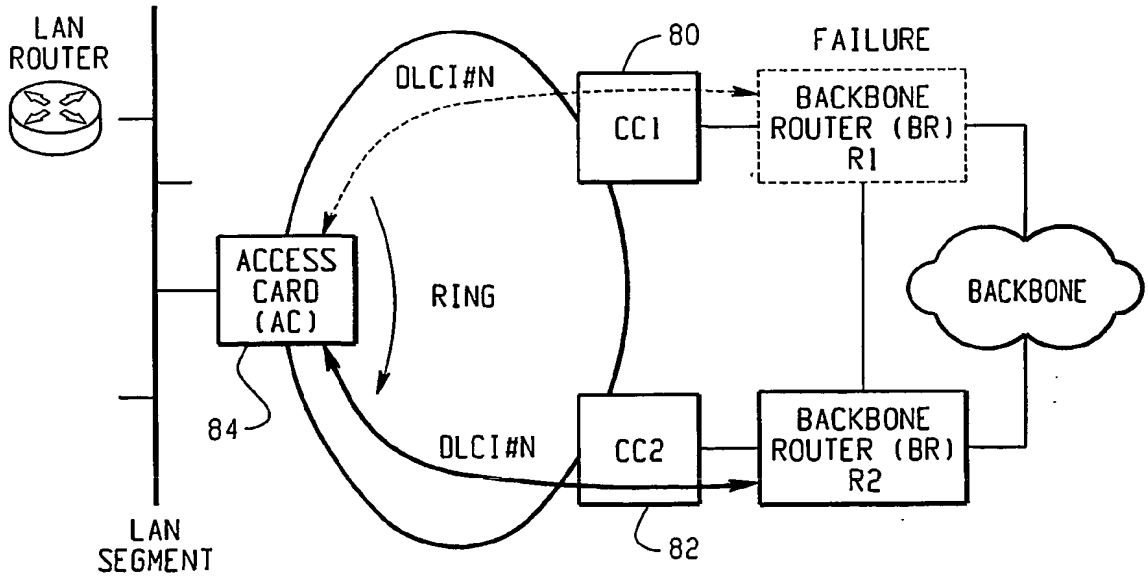

LAN
ROUTER
80
FAILURE
DLCI#N
CC1
BACKBONE
ROUTER (BR)
R1
ACCESS
CARD
(AC)
RING
BACKBONE
84
DLCI#N
CC2
BACKBONE
ROUTER (BR)
R2
82
LAN
SEGMENT

Fig. 13

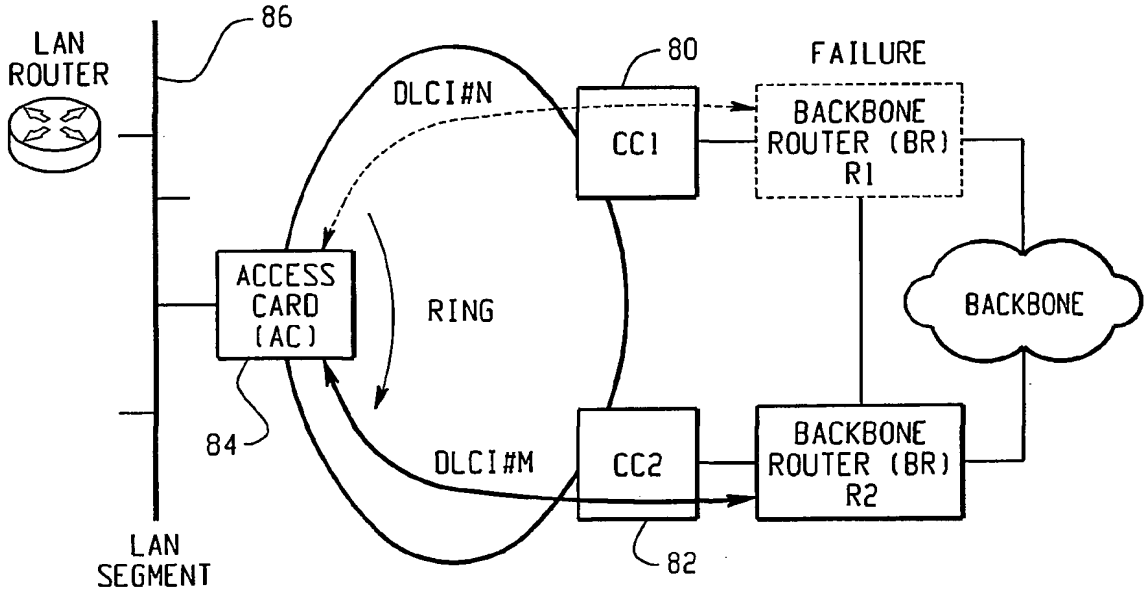

LAN
ROUTER
86
80
FAILURE
DLCI#N
CC1
BACKBONE
ROUTER (BR)
R1
ACCESS
CARD
(AC)
RING
BACKBONE
84
DLCI#M
CC2
BACKBONE
ROUTER (BR)
R2
LAN
SEGMENT
82

Fig. 14

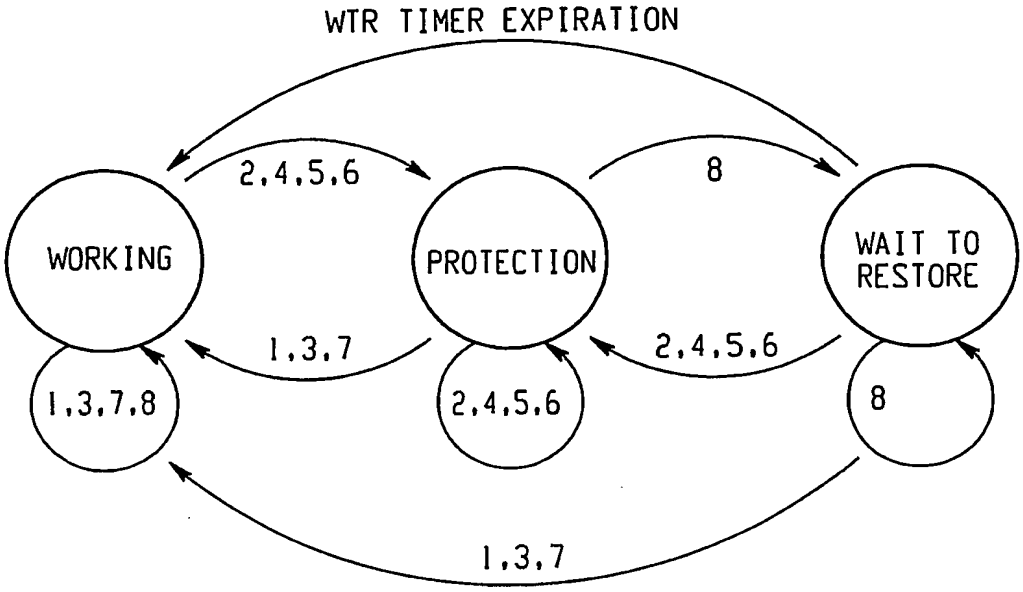

WTR TIMER EXPIRATION
2,4,5,6
8
WORKING
PROTECTION
WAIT TO RESTORE
1,3,7
2,4,5,6
1,3,7,8
2,4,5,6
8
1,3,7

Fig. 15

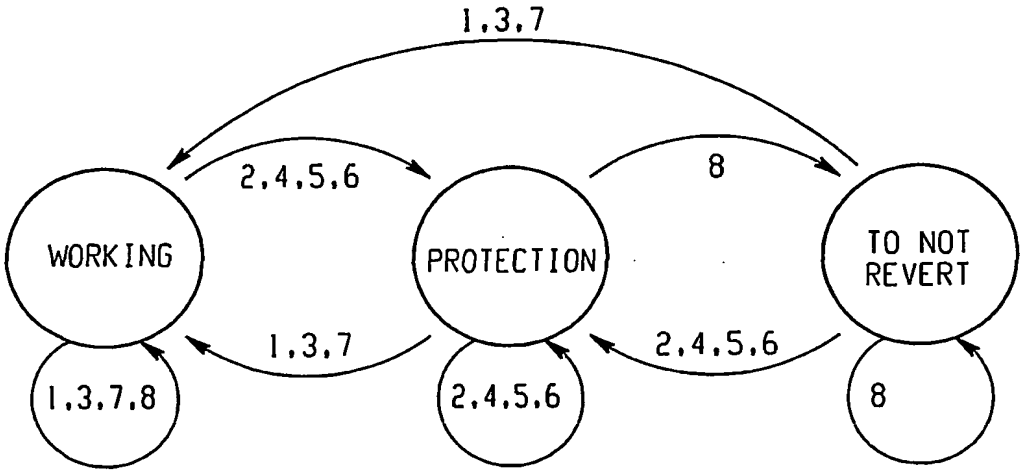

1,3,7
2,4,5,6
8
WORKING
PROTECTION
TO NOT REVERT
1,3,7
2,4,5,6
1,3,7,8
2,4,5,6
8

Fig. 16

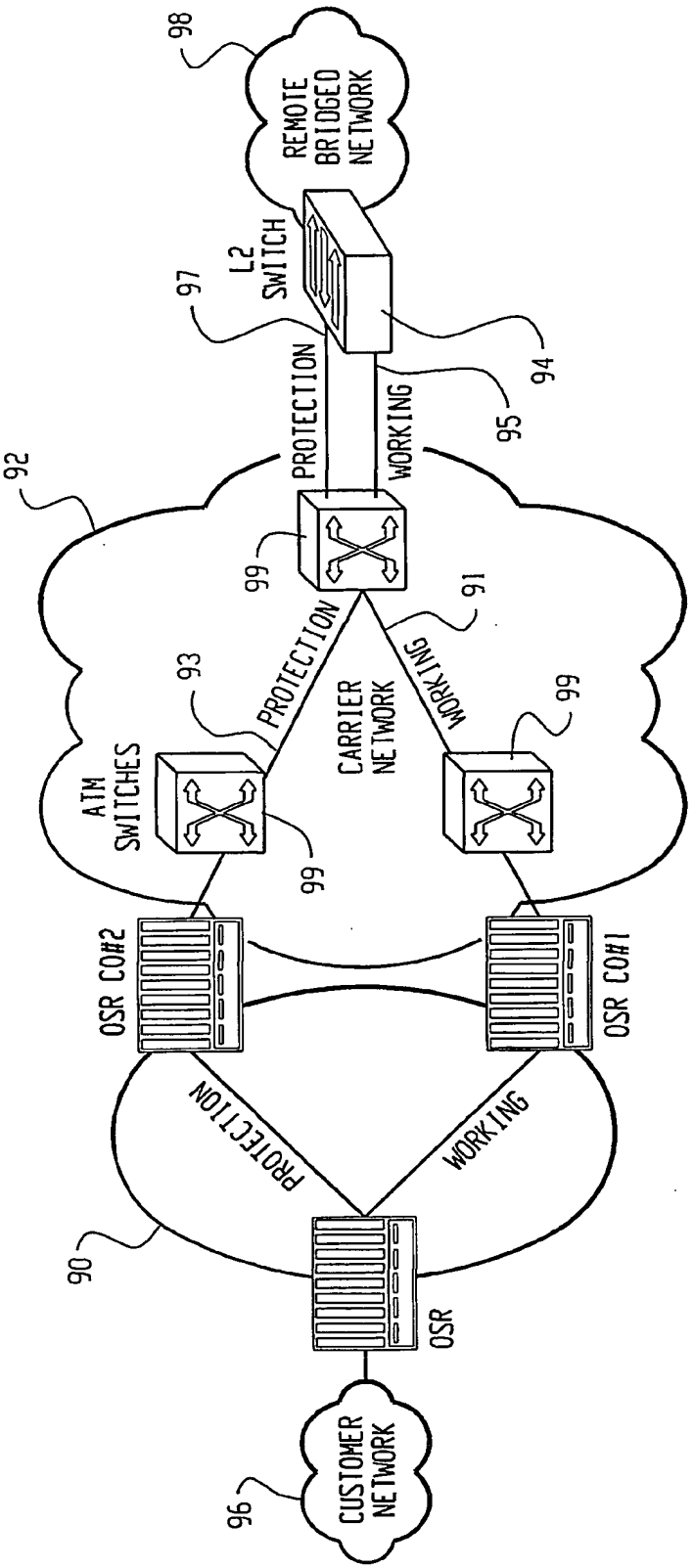

98
REMOTE BRIDGED NETWORK
L2 SWITCH
97
94
95
PROTECTION
WORKING
92
99
91
93
PROTECTION
WORKING
CARRIER NETWORK
ATM SWITCHES
99
99
OSR CO#2
OSR CO#1
PROTECTION
WORKING
90
OSR
CUSTOMER NETWORK
96

Fig. 17

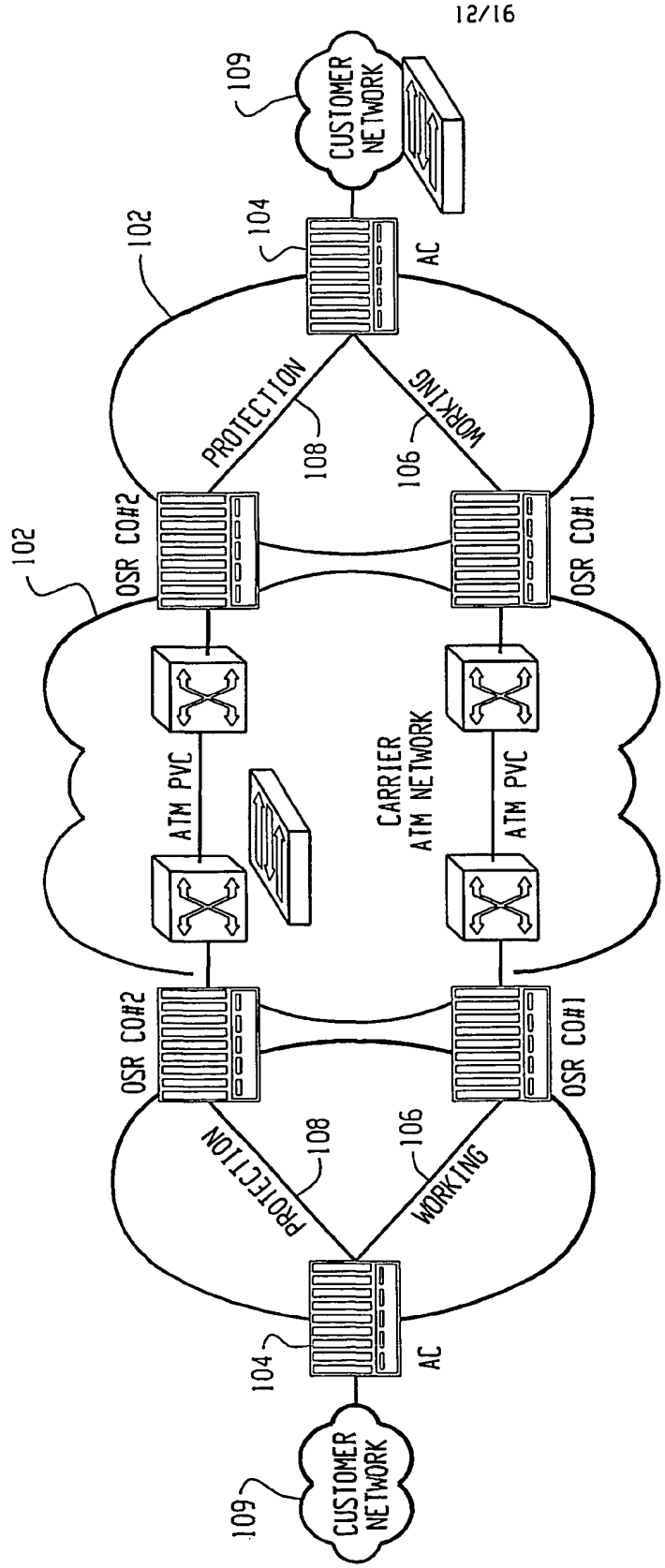

109
CUSTOMER NETWORK
104
AC
102
PROTECTION
108
WORKING
106
OSR CO#2
OSR CO#1
102
ATM PVC
CARRIER ATM NETWORK
ATM PVC
OSR CO#2
OSR CO#1
PROTECTION
108
106
WORKING
104
AC
109
CUSTOMER NETWORK

Fig. 18

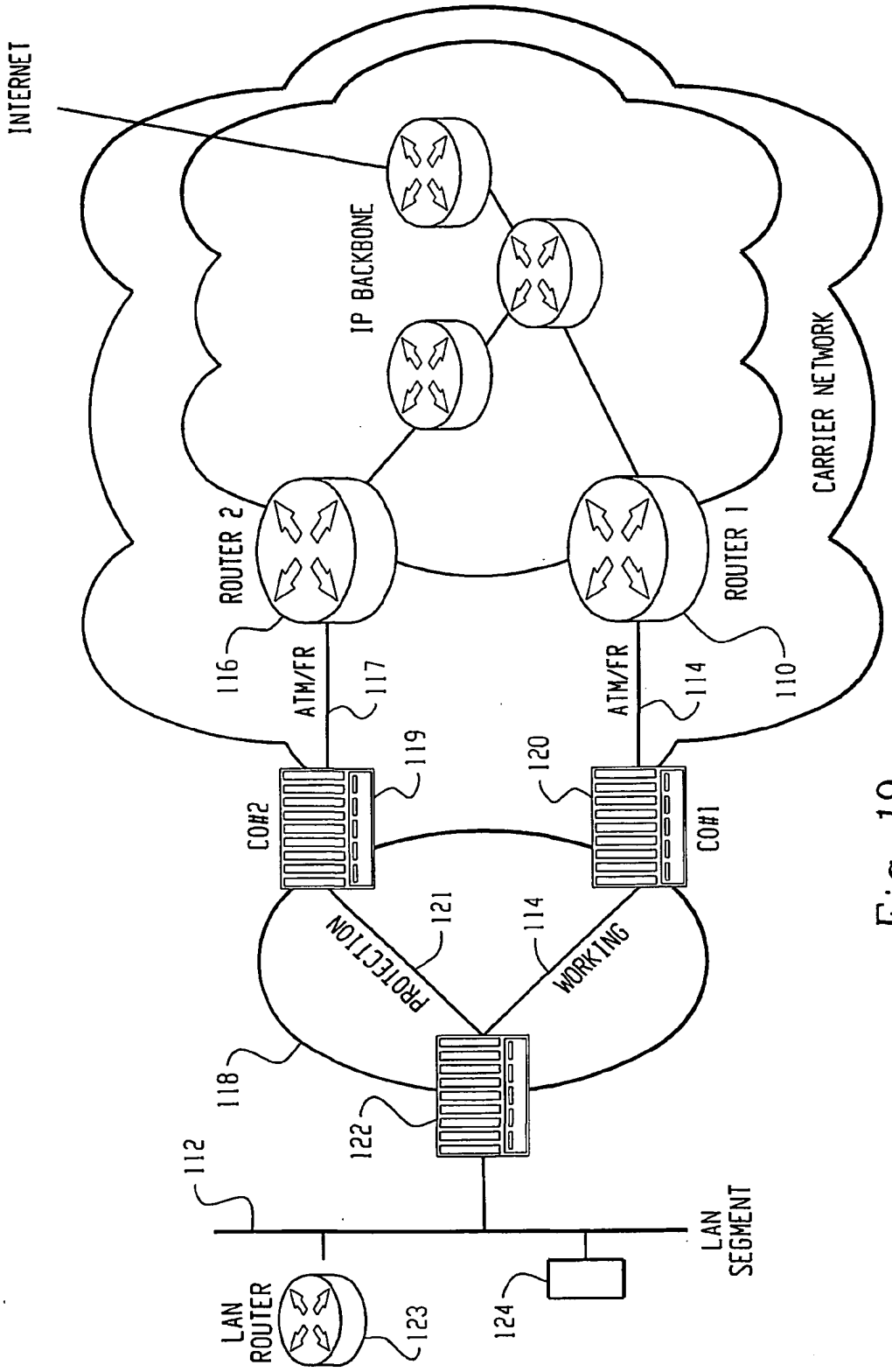

INTERNET
IP BACKBONE
CARRIER NETWORK
ROUTER 2
ROUTER 1
116
ATM/FR
117
ATM/FR
114
110
119
120
CO#2
CO#1
PROTECTION
121
114
WORKING
118
122
112
LAN SEGMENT
LAN ROUTER
123
124

Fig. 19

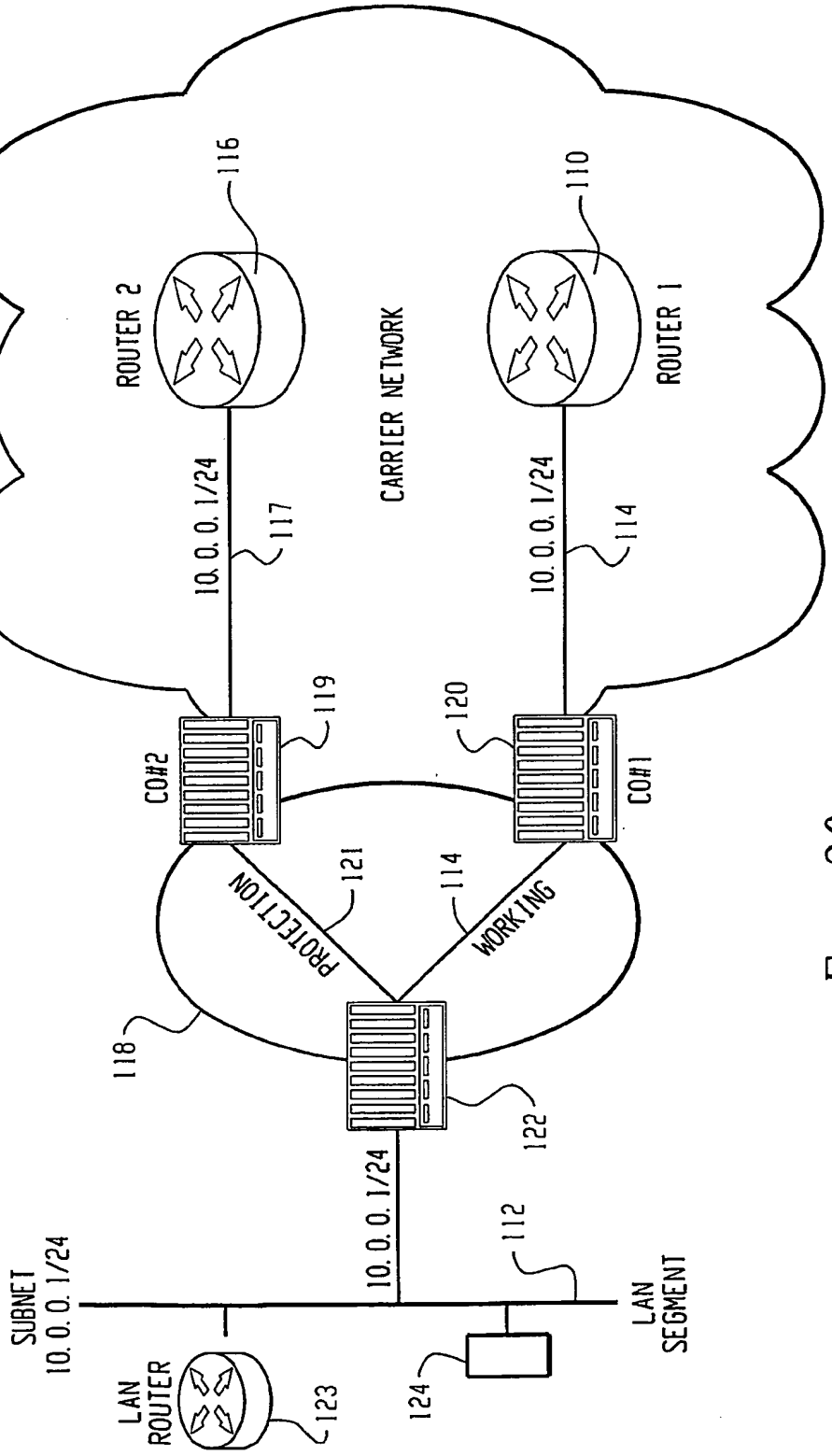

ROUTER 2
116
ROUTER 1
110
CARRIER NETWORK
10.0.0.1/24
117
10.0.0.1/24
114
119
120
CO#2
CO#1
PROTECTION
121
114
WORKING
118
122
10.0.0.1/24
112
SUBNET
10.0.0.1/24
LAN
SEGMENT
LAN
ROUTER
123
124

Fig. 20

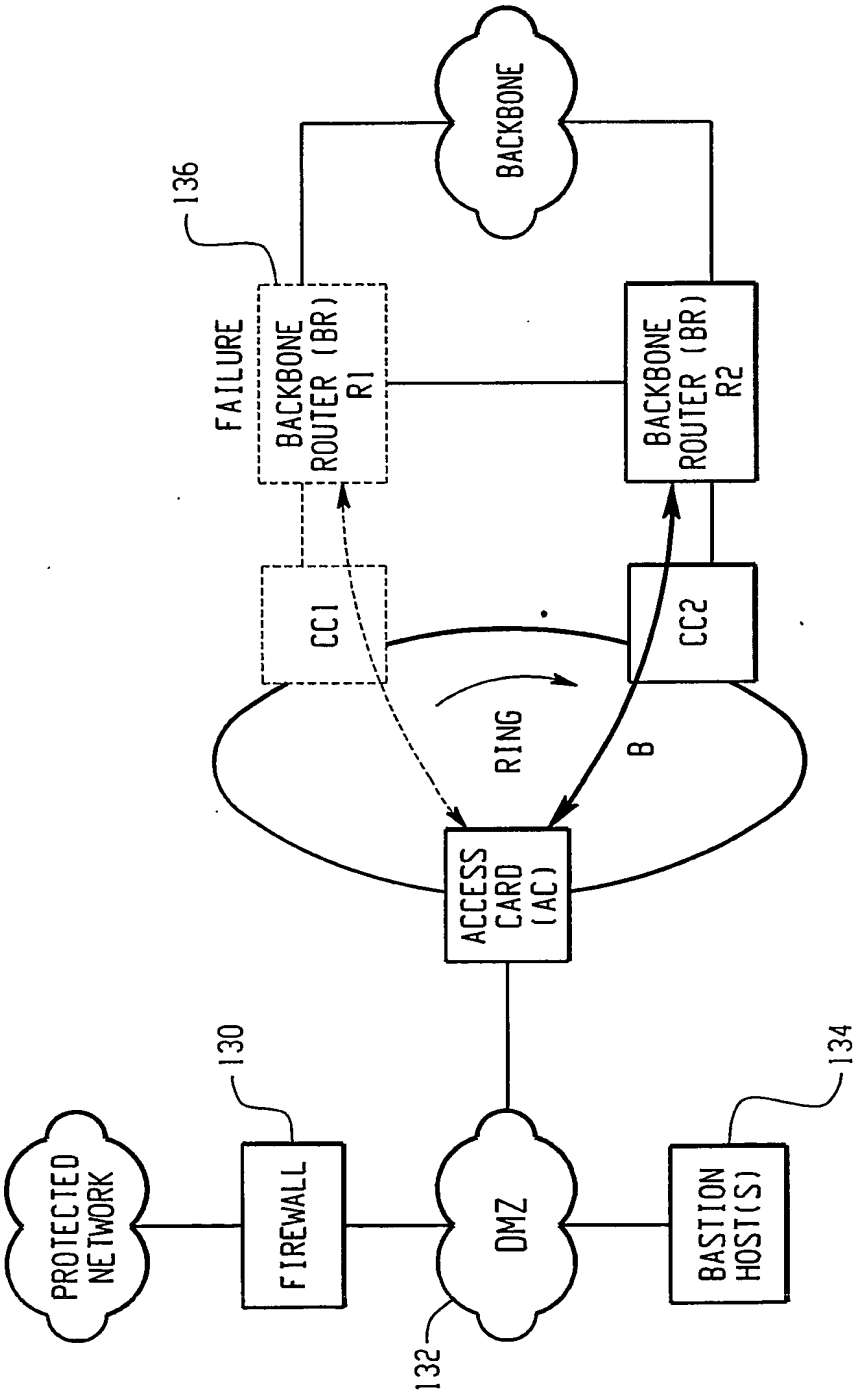

BACKBONE
136
FAILURE
BACKBONE ROUTER (BR) R1
BACKBONE ROUTER (BR) R2
CC1
CC2
RING
B
ACCESS CARD (AC)
130
134
PROTECTED NETWORK
FIREWALL
DMZ
BASTION HOST(S)
132

Fig. 21

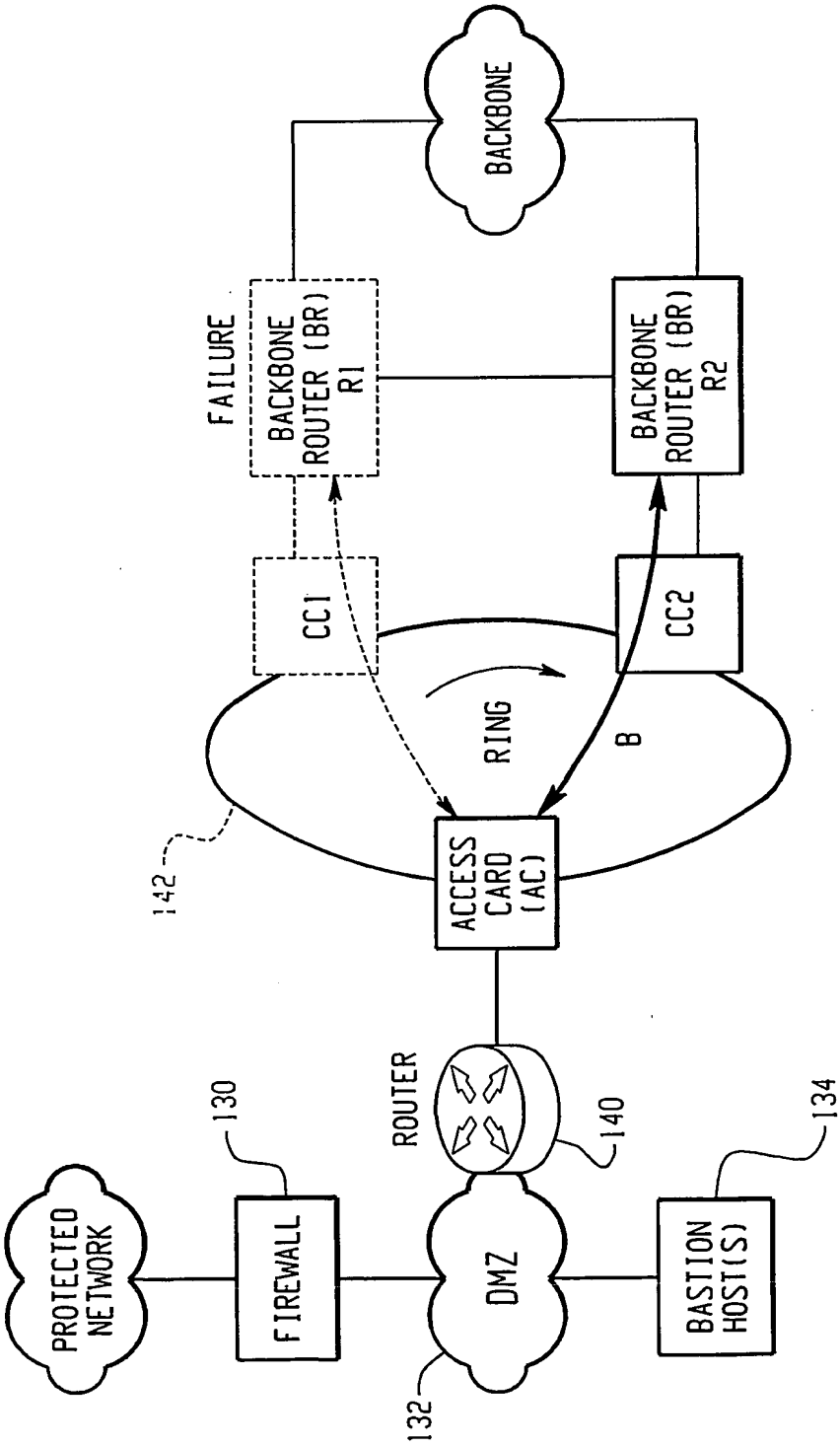

BACKBONE
FAILURE
BACKBONE ROUTER (BR) R1
BACKBONE ROUTER (BR) R2
CC1
CC2
RING
B
142
ACCESS CARD (AC)
ROUTER
130
140
134
PROTECTED NETWORK
FIREWALL
DMZ
BASTION HOST(S)
132

Fig. 22